

15.12.2004

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

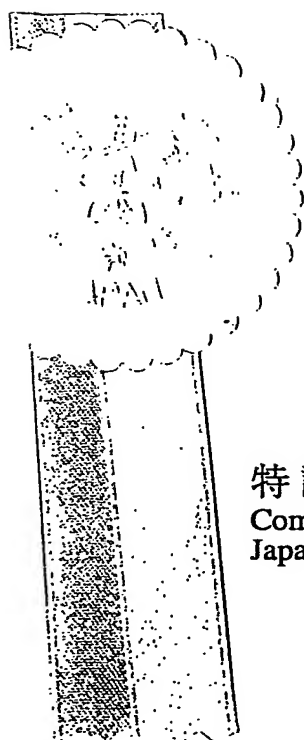
別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日            2 0 0 3 年 1 2 月 1 7 日  
Date of Application:

出 願 番 号            特 願 2 0 0 3 - 4 1 9 7 6 5  
Application Number:  
[ST. 10/C]:            [ J P 2 0 0 3 - 4 1 9 7 6 5 ]

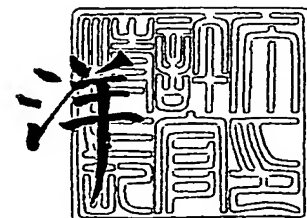
出      願      人            松 下 電 器 産 業 株 式 会 社  
Applicant(s):



特許庁長官  
Commissioner,  
Japan Patent Office

2 0 0 5 年   1 月 2 7 日

小 川



【書類名】 特許願  
【整理番号】 2022550300  
【あて先】 特許庁長官殿  
【国際特許分類】 G09L 1/00  
【発明者】  
    【住所又は居所】 大阪府門真市大字門真 1006 番地 松下電器産業株式会社内  
    【氏名】 野仲 真佐男  
【発明者】  
    【住所又は居所】 大阪府門真市大字門真 1006 番地 松下電器産業株式会社内  
    【氏名】 布田 裕一  
【発明者】  
    【住所又は居所】 大阪府門真市大字門真 1006 番地 松下電器産業株式会社内  
    【氏名】 大森 基司  
【発明者】  
    【住所又は居所】 大阪府門真市大字門真 1006 番地 松下電器産業株式会社内  
    【氏名】 山田 茂  
【発明者】  
    【住所又は居所】 大阪府門真市大字門真 1006 番地 松下電器産業株式会社内  
    【氏名】 井上 哲也  
【発明者】  
    【住所又は居所】 愛知県名古屋市中区栄 2 丁目 6 番 1 号白川ビル別館 5 F 株式会  
    社松下電器情報システム名古屋研究所内  
    【氏名】 熊崎 洋児  
【特許出願人】  
    【識別番号】 000005821  
    【氏名又は名称】 松下電器産業株式会社  
【代理人】  
    【識別番号】 100109210  
    【弁理士】  
    【氏名又は名称】 新居 広守  
【手数料の表示】  
    【予納台帳番号】 049515  
    【納付金額】 21,000円  
【提出物件の目録】  
    【物件名】 特許請求の範囲 1  
    【物件名】 明細書 1  
    【物件名】 図面 1  
    【物件名】 要約書 1  
    【包括委任状番号】 0213583

## 【書類名】特許請求の範囲

## 【請求項 1】

コンテンツを配信するコンテンツ配信システムであって、

前記コンテンツ配信システムは、前記コンテンツを暗号化して配信するサーバと、暗号化された前記コンテンツを受信、復号化する複数の出力装置と、から構成され、前記サーバと前記出力装置のそれぞれは通信路を介して通信可能であって、さらに、各出力装置は、所定の鍵割当方法により個別に割り当てられた割当ノード復号化鍵群を保持しており、

前記鍵割当方法は、一以上の木構造を用いており、各々の前記木構造は複数のノードから構成され、前記複数のノードは複数の階層（第0階層から第 $n$ 階層： $n$ は1以上の自然数）により分類され、ただし、前記第0階層は一つの前記ノードから構成され、前記木構造の全ての前記ノードに一以上のノード暗号化鍵及び対応するノード復号化鍵の組を設定し、前記第 $i$ 階層（ $i$ は1から $n$ までの自然数）の前記ノードは、前記第0階層から前記第 $i-1$ 階層のいずれか一つの前記ノードである親ノードと線で結ばれており、前記第 $n$ 階層の前記ノード、および、前記第 $j$ 階層（ $j$ は1から $n-1$ までの自然数）の前記ノードであり、前記第 $j+1$ 階層から前記第 $n$ 階層のいずれの前記ノードにも線で結ばれていない前記ノードを末端ノードとし、前記末端ノードに対して、関連ノード集合は、前記末端ノードと、前記末端ノードの親ノードと、前記関連ノード集合に属するノードの親ノードから成り、前記関連ノード集合に属するノードに設定された前記ノード復号化鍵を割当ノード復号化鍵群とし、ノード暗号化鍵群を、全ての前記ノードに設定された前記ノード暗号化鍵とし、前記出力装置に前記末端ノードのいずれかを対応づけ、前記末端ノードの前記関連ノード集合に対応する前記割当ノード復号化鍵群を割り当てる方法であり、

前記サーバは、

前記鍵割当方法により予め与えられる前記ノード暗号化鍵群を保持する鍵情報格納部と

、  
前記ノード暗号化鍵群の中から一以上の前記ノード暗号化鍵を選定し選定ノード暗号化鍵群とし、前記選定ノード暗号化鍵群は、少なくとも前記末端ノードに設定されている前記ノード暗号化鍵を含み、かつ、前記末端ノード以外の前記ノードに設定されている前記ノード暗号化鍵を含み、前記選定ノード暗号化鍵群の中の前記ノード暗号化鍵の各々を用いて、予め与えられるコンテンツ復号化鍵を暗号化することによって、暗号化コンテンツ鍵群を生成するコンテンツ鍵選択部と、

外部から前記コンテンツを受信する入力部と、

前記コンテンツ復号化鍵に対応し予め与えられるコンテンツ暗号化鍵に基づき前記コンテンツを暗号化する暗号化部と、

前記暗号化コンテンツ及び前記暗号化コンテンツ鍵群を前記出力装置に配信する送信部と、を備え、

前記出力装置は、

前記暗号化コンテンツ及び前記暗号化コンテンツ鍵群を受信する第一受信部と、

前記鍵割当方法により予め与えられる前記割当ノード復号化鍵群を保持するノード鍵格納部と、

前記割当ノード復号化鍵群及び前記暗号化コンテンツ鍵群に基づき前記コンテンツ復号化鍵を取得する復号化鍵取得部と、

前記コンテンツ復号化鍵に基づき前記暗号化コンテンツを復号化する第一復号化部と、を備えることを特徴とする、コンテンツ配信システム。

## 【請求項 2】

前記サーバは、さらに、複数の前記コンテンツを受信するとし、外部から前記コンテンツを受信した際に、前回前記コンテンツを暗号化する際に用いた一以上の前記コンテンツ暗号化鍵及び対応する前記コンテンツ復号化鍵の組とは異なる一以上の前記コンテンツ暗号化鍵及び対応する前記コンテンツ復号化鍵の組を新たに生成するコンテンツ鍵生成部を備えることを特徴とする、請求項 1 に記載のコンテンツ配信システム。

## 【請求項 3】

前記サーバは、さらに、複数の前記コンテンツを受信するとし、前記コンテンツ鍵選択部は、さらに、前記サーバが外部から前記コンテンツを受信した際に、前回選定した前記末端ノードとは異なる前記末端ノードに設定されている前記ノード暗号化鍵を含む前記選定ノード暗号化鍵群を新たに作成することを特徴とする、請求項1または請求項2に記載のコンテンツ配信システム。

【請求項4】

前記サーバは、さらに、前記割当ノード復号化鍵群における前記ノード暗号化鍵の鍵選定情報を複数保持する鍵選定情報格納部を備え、

前記コンテンツ鍵選択部は、前記鍵選定情報格納部の保持している複数の前記鍵選定情報を基に、前記選定ノード暗号化鍵群を作成することを特徴とする、請求項1から請求項3のいずれか1項に記載のコンテンツ配信システム。

【請求項5】

前記サーバ及び前記出力装置は、さらに、前記選定ノード暗号化鍵群における前記ノード暗号化鍵の鍵選定情報と前記鍵選定情報を識別する鍵選定識別子を対応付けて複数保持している鍵選定情報格納部を備え、

前記コンテンツ鍵選択部は、前記鍵選定情報格納部の保持している複数の前記鍵選定情報のいずれかの前記鍵選定情報を基に前記選定ノード暗号化鍵群を作成し、基にした前記鍵選定情報に対応する前記鍵選定識別子を前記送信部へ出力し、

前記送信部は、前記暗号化コンテンツ及び前記暗号化コンテンツ鍵群及び前記鍵選定識別子を前記出力装置に配信し、

前記第一受信部は、前記暗号化コンテンツ及び前記暗号化コンテンツ鍵群及び前記鍵選定識別子を受信し、

前記復号化鍵取得部は、前記鍵選定情報格納部の保持している複数の前記鍵選定情報を用いて、前記割当ノード復号化鍵群及び前記暗号化コンテンツ鍵群及び前記鍵選定識別子を基に、前記コンテンツ復号化鍵を取得することを特徴とする、請求項1から請求項3のいずれか1項に記載のコンテンツ配信システム。

【請求項6】

前記コンテンツ鍵選択部は、前記鍵選定情報格納部が保持している複数の前記鍵選定情報の中からランダムに一つの前記鍵選定情報を選択し、選択された前記鍵選定情報を基に前記選定ノード暗号化鍵群を作成することを特徴とする、請求項4または請求項5に記載のコンテンツ配信システム。

【請求項7】

前記コンテンツ鍵選択部は、前記鍵選定情報格納部が保持している複数の前記鍵選定情報の中の前記鍵選定情報を周期的に一つ選択し、選択された前記鍵選定情報を基に選定ノード暗号化鍵群を作成することを特徴とする、請求項4または請求項5に記載のコンテンツ配信システム。

【請求項8】

前記鍵割当方法における木構造は、N分木（Nは2以上の自然数）であることを特徴とする、請求項1から請求項7のいずれか1項に記載のコンテンツ配信システム。

【請求項9】

前記コンテンツ配信システムは、さらに、前記通信路を介して前記出力装置のそれぞれとサーバに接続され、前記ノード暗号化鍵群及び複数の前記割当ノード復号化鍵群を配信する鍵発行センタを備え、

前記鍵発行センタは、

前記鍵割当方法に基づき、前記ノード暗号化鍵群及び複数の割当ノード復号化鍵群を生成するノード鍵生成部と、

前記ノード暗号化鍵群を前記サーバに送信する第一送信部と、

複数の前記割当ノード復号化鍵群と複数の前記出力装置の対応情報を保持する出力装置対応情報格納部と、

前記対応情報に基づき複数の前記割当ノード復号化鍵群を前記それぞれの出力装置に配

信する第二送信部と、を備え

前記サーバは、

受信した前記ノード暗号化鍵群を前記鍵情報格納部に格納する受信部を備え、

前記出力装置は、

受信した前記割当ノード復号化鍵群を前記ノード鍵格納部へ格納する第二受信部を備えることを特徴とする、請求項 1 から請求項 8 のいずれか 1 項に記載のコンテンツ配信システム。

【請求項 10】

前記コンテンツ配信システムは、さらに、前記通信路を介して前記出力装置のそれぞれとサーバに接続され、前記ノード暗号化鍵群及び鍵更新情報を配信する鍵発行センタを備え、

前記鍵発行センタは、

予め各々の前記出力装置に与えられる個別鍵を保持する出力装置対応情報格納部と、各々の前記出力装置に与えられる前記個別鍵を基に各々の前記出力装置に割り当てられた前記割当ノード復号化鍵群を暗号化し、鍵更新情報を生成する第一暗号化部と、

前記鍵更新情報を前記出力装置へ配信する第二送信部とを備え、

前記出力装置は、前記鍵更新情報を受信する第二受信部と、

予め与えられる前記個別鍵を保持する個別鍵格納部と、

前記個別鍵に基づき受信した前記鍵更新情報の復号化を行い、復号化された前記割当ノード復号化鍵群を前記ノード鍵格納部へ格納する第二復号化部と、を備えることを特徴とする、請求項 1 から請求項 8 のいずれか 1 項に記載のコンテンツ配信システム。

【請求項 11】

前記出力装置対応情報格納部は、さらに、各々の前記出力装置に対応付けられている出力装置識別子と前記割当ノード復号化鍵群の対応情報を保持し、

前記鍵発行センタは、外部から前記出力装置識別子を受信した場合に、前記出力装置識別子を基に、前記出力装置対応情報格納部の保持している前記対応情報を更新し、さらに、前記ノード鍵生成要求を前記ノード鍵生成部へ出力する対応情報更新部を備え、

前記ノード鍵生成部は、前記ノード鍵生成要求を受信した場合に、前記鍵割当方法に基づき、前記ノード暗号化鍵群及び複数の割当ノード復号化鍵群を生成することを特徴とする、請求項 10 に記載のコンテンツ配信システム。

【請求項 12】

前記ノード鍵生成部は、前記鍵割当方法に基づき、前記ノード暗号化鍵群及び複数の割当ノード復号化鍵群を生成した場合、前記第一暗号化部へ鍵更新情報生成要求を出力し、

前記第一暗号化部は、前記鍵更新情報生成要求を受信した場合、各々の前記出力装置に与えられる前記個別鍵を基に各々の前記出力装置に割り当てられた前記割当ノード復号化鍵群を暗号化し、鍵更新情報を生成することを特徴とする、請求項 10 または請求項 11 に記載のコンテンツ配信システム。

【請求項 13】

コンテンツを暗号化して配信するサーバと、通信路を介して前記サーバに接続され、前記コンテンツを受信する出力装置と、を備えるコンテンツ配信システムにおける出力装置であって、

各出力装置は、さらに、所定の鍵割当方法により個別に割り当てられた割当ノード復号化鍵群を保持しており、

前記サーバ及び前記出力装置は、さらに、前記割当ノード復号化鍵群における前記ノード暗号化鍵の鍵選定情報と前記鍵選定情報を識別する鍵選定識別子に対応付けて複数保持している鍵選定情報格納部を備え、

前記鍵割当方法は、一以上の木構造を用いており、各々の前記木構造は複数のノードから構成され、前記複数のノードは複数の階層（第 0 階層から第  $n$  階層： $n$  は 1 以上の自然数）により分類され、ただし、前記第 0 階層は一つの前記ノードから構成され、前記木構造の全ての前記ノードに一以上のノード暗号化鍵及び対応するノード復号化鍵の組を設定

し、前記第  $i$  階層 ( $i$  は 1 から  $n$  までの自然数) の前記ノードは、前記第 0 階層から前記第  $i-1$  階層のいずれか一つの前記ノードである親ノードと線で結ばれており、前記第  $n$  階層の前記ノード、および、前記第  $j$  階層 ( $j$  は 1 から  $n-1$  までの自然数) の前記ノードであり、前記第  $j+1$  階層から前記第  $n$  階層のいずれの前記ノードにも線で結ばれていない前記ノードを末端ノードとし、前記末端ノードに対して、関連ノード集合は、前記末端ノードと、前記末端ノードの親ノードと、前記関連ノード集合に属するノードの親ノードから成り、前記関連ノード集合に属するノードに設定された前記ノード復号化鍵を割当ノード復号化鍵群とし、ノード暗号化鍵群を、全ての前記ノードに設定された前記ノード暗号化鍵とし、前記出力装置に前記末端ノードのいずれかを対応づけ、前記末端ノードの前記関連ノード集合に対応する前記割当ノード復号化鍵群を割り当て方法であり、

前記出力装置は、

外部から前記暗号化コンテンツ及び前記暗号化コンテンツ鍵群及び前記鍵選定識別子を受信する第一受信部と、

前記鍵割当方法により予め与えられる前記割当ノード復号化鍵群を保持するノード鍵格納部と、

前記鍵選定情報格納部の保持している複数の前記鍵選定情報を用いて、前記割当ノード復号化鍵群及び前記暗号化コンテンツ鍵群及び前記鍵選定情報識別子を基に、前記コンテンツ復号化鍵を取得する復号化鍵取得部と、

前記コンテンツ復号化鍵に基づき前記暗号化コンテンツを復号化する第一復号化部と、を備えることを特徴とする、出力装置。

#### 【請求項 14】

前記鍵割当方法における木構造は、 $N$ 分木 ( $N$  は 2 以上の自然数) であることを特徴とする、請求項 13 に記載の出力装置。

#### 【請求項 15】

前記コンテンツ配信システムは、さらに、前記通信路を介して前記出力装置のそれぞれとサーバに接続され、前記ノード暗号化鍵群及び複数の前記割当ノード復号化鍵群を配信する鍵発行センタを備え、

さらに、外部から受信した前記割当ノード復号化鍵群を前記ノード鍵格納部へ格納する第二受信部と、を備えることを特徴とする、請求項 13 または請求項 14 に記載の出力装置。

#### 【請求項 16】

前記コンテンツ配信システムは、さらに、前記通信路を介して前記出力装置のそれぞれとサーバに接続され、前記ノード暗号化鍵群及び鍵更新情報を配信する鍵発行センタを備え、

さらに、外部から前記鍵更新情報を受信する第二受信部と、

予め与えられる個別鍵を保持する個別鍵格納部と、

前記個別鍵に基づき受信した前記鍵更新情報の復号化を行い、復号化された前記割当ノード復号化鍵群を前記ノード鍵格納部へ格納する第二復号化部と、を備えることを特徴とする、請求項 13 または請求項 14 に記載のコンテンツ配信システム。

#### 【請求項 17】

コンテンツを暗号化して配信するサーバと、通信路を介して前記サーバに接続され、前記コンテンツを受信する処理をコンピュータに実行させるプログラムであって、所定の鍵割当方法により個別に割り当てられた割当ノード復号化鍵群を保持しており、さらに、前記割当ノード復号化鍵群における複数の前記ノード暗号化鍵の鍵選定情報と前記鍵選定情報を識別する鍵選定識別子の対応情報を保持しており、

前記鍵割当方法は、一以上の木構造を用いており、各々の前記木構造は複数のノードから構成され、前記複数のノードは複数の階層 (第 0 階層から第  $n$  階層:  $n$  は 1 以上の自然数) により分類され、ただし、前記第 0 階層は一つの前記ノードから構成され、前記木構造の全ての前記ノードに一以上のノード暗号化鍵及び対応するノード復号化鍵の組を設定し、前記第  $i$  階層 ( $i$  は 1 から  $n$  までの自然数) の前記ノードは、前記第 0 階層から前記

第  $i-1$  階層のいずれか一つの前記ノードである親ノードと線で結ばれており、前記第  $n$  階層の前記ノード、および、前記第  $j$  階層 ( $j$  は 1 から  $n-1$  までの自然数) の前記ノードであり、前記第  $j+1$  階層から前記第  $n$  階層のいずれの前記ノードにも線で結ばれていない前記ノードを末端ノードとし、前記末端ノードに対して、関連ノード集合は、前記末端ノードと、前記末端ノードの親ノードと、前記関連ノード集合に属するノードの親ノードから成り、前記関連ノード集合に属するノードに設定された前記ノード復号化鍵を割当ノード復号化鍵群とし、ノード暗号化鍵群を、全ての前記ノードに設定された前記ノード暗号化鍵とし、前記出力装置に前記末端ノードのいずれかを対応づけ、前記末端ノードの前記関連ノード集合に対応する前記割当ノード復号化鍵群を割り当てる方法であり、

外部から前記暗号化コンテンツ及び前記暗号化コンテンツ鍵群及び前記鍵選定識別子を受信するステップと、

複数の前記鍵選定情報を用いて、前記割当ノード復号化鍵群及び前記暗号化コンテンツ鍵群及び前記鍵選定情報識別子を基に、前記コンテンツ復号化鍵を取得するステップと、

前記コンテンツ復号化鍵に基づき前記暗号化コンテンツを復号化するステップと、をコンピュータに実行させることを特徴とする、プログラム。

【請求項 18】

請求項 17 に記載のプログラムを記録した媒体。

【請求項 19】

さらに、前記鍵割当方法における木構造は、 $N$  分木 ( $N$  は 2 以上の自然数) であることを特徴とする、請求項 17 に記載のプログラム。

【請求項 20】

請求項 19 に記載のプログラムを記録した媒体。

【請求項 21】

さらに、前記通信路を介して前記プログラムと前記サーバに接続され、前記ノード暗号化鍵群及び複数の前記割当ノード復号化鍵群を配信する鍵発行センタを備え、

さらに、外部から前記割当ノード復号化鍵群を受信するステップと、をコンピュータに実行させることを特徴とする、請求項 17 または請求項 19 に記載のプログラム。

【請求項 22】

請求項 21 に記載のプログラムを記録した媒体。

【請求項 23】

さらに、前記通信路を介して前記プログラムと前記サーバに接続され、前記ノード暗号化鍵群及び鍵更新情報を配信する鍵発行センタを備え、

さらに、外部から前記鍵更新情報を受信するステップと、予め与えられる個別鍵に基づき受信した前記鍵更新情報の復号化を行うステップと、をコンピュータに実行させることを特徴とする、請求項 17 または請求項 19 に記載のプログラム。

【請求項 24】

請求項 23 に記載のプログラムを記録した媒体。

【請求項 25】

コンテンツを配信するコンテンツ配信方法であって、

前記コンテンツ配信方法は、所定の鍵割当方法を基に予め与えられたノード暗号化鍵群を用いて前記コンテンツを暗号化して配信するコンテンツ配信ステップと、前記鍵割当方法を基に予め与えられた割当ノード復号化鍵群を用いて暗号化された前記コンテンツを復号化するコンテンツ受信ステップと、から構成され、

前記鍵割当方法は、一以上の木構造を用いており、各々の前記木構造は複数のノードから構成され、前記複数のノードは複数の階層 (第 0 階層から第  $n$  階層:  $n$  は 1 以上の自然数) により分類され、ただし、前記第 0 階層は一つの前記ノードから構成され、前記木構造の全ての前記ノードに一以上のノード暗号化鍵及び対応するノード復号化鍵の組を設定し、前記第  $i$  階層 ( $i$  は 1 から  $n$  までの自然数) の前記ノードは、前記第 0 階層から前記第  $i-1$  階層のいずれか一つの前記ノードである親ノードと線で結ばれており、前記第  $n$  階層の前記ノード、および、前記第  $j$  階層 ( $j$  は 1 から  $n-1$  までの自然数) の前記ノード

ドであり、前記第  $j+1$  階層から前記第  $n$  階層のいずれの前記ノードにも線で結ばれていない前記ノードを末端ノードとし、前記末端ノードに対して、関連ノード集合は、前記末端ノードと、前記末端ノードの親ノードと、前記関連ノード集合に属するノードの親ノードから成り、前記関連ノード集合に属するノードに設定された前記ノード復号化鍵を割当ノード復号化鍵群とし、ノード暗号化鍵群を、全ての前記ノードに設定された前記ノード暗号化鍵とし、前記コンテンツ受信ステップに前記末端ノードのいずれかを対応づけ、前記末端ノードの前記関連ノード集合に対応する前記割当ノード復号化鍵群を割り当てる方法であり、

前記コンテンツ配信ステップは、

前記鍵割当方法により予め与えられる前記ノード暗号化鍵群の中から一以上の前記ノード暗号化鍵を選定し選定ノード暗号化鍵群とし、前記選定ノード暗号化鍵群は、少なくとも前記末端ノードに設定されている前記ノード暗号化鍵を含み、かつ、前記末端ノード以外の前記ノードに設定されている前記ノード暗号化鍵を含み、前記選定ノード暗号化鍵群の中の前記ノード暗号化鍵の各々を用いて、予め与えられるコンテンツ復号化鍵を暗号化することによって、暗号化コンテンツ鍵群を生成するステップと、

外部から前記コンテンツを受信するステップと、

前記コンテンツ復号化鍵に対応し予め与えられるコンテンツ暗号化鍵に基づき前記コンテンツを暗号化するステップと、

前記暗号化コンテンツ及び前記暗号化コンテンツ鍵群を前記出力装置に配信するステップと、を含み、

前記コンテンツ受信ステップは、前記暗号化コンテンツ及び前記暗号化コンテンツ鍵群を受信するステップと、前記鍵割当方法により予め与えられる前記割当ノード復号化鍵群及び前記暗号化コンテンツ鍵群に基づき前記コンテンツ復号化鍵を取得するステップと、前記コンテンツ復号化鍵に基づき前記暗号化コンテンツを復号化するステップと、を含むことを特徴とする、コンテンツ配信方法。



【書類名】明細書

【発明の名称】コンテンツ配信システム

【技術分野】

【0001】

本発明は、映画や音楽などのデジタルコンテンツを複数の出力装置に暗号化して配信するコンテンツ配信システムに関し、特に、暗号化されたコンテンツを出力装置で復号化する際に用いる鍵を出力装置毎に個別にすることで、もし出力装置に割り当てられている鍵が漏洩しても、その漏洩元の出力装置を追跡可能な技術に関する。

【背景技術】

【0002】

ADSLや光ファイバーなどに代表される高速通信路の普及に伴い、デジタル化された音楽や映像等のコンテンツを通信路を介して提供するサービスが盛んに行われるようになった。このようなサービスの普及に伴い、不正コピーなどに代表されるコンテンツ不正利用を防止する著作権保護方式が必要となってきた。一般に、このコンテンツ不正利用を防止する著作権保護方式には、暗号技術が用いられる。つまり、あるコンテンツ暗号化鍵を用いてデジタルコンテンツを暗号化して通信路を介して配布し、そのコンテンツ暗号化鍵に対応するコンテンツ復号化鍵を与えられている出力装置のみが、暗号化されたコンテンツを復号化して、元のデジタルコンテンツの再生を行うことが出来るというものである。

【0003】

ところで、通常、出力装置に与えられているコンテンツ復号化鍵は秘密に保持されるが、端末の不正解析などによって、攻撃者が全装置共通に与えられているコンテンツ復号化鍵を取得する可能性がある。ある端末に与えられているコンテンツ復号化鍵が一旦漏洩してしまうと、攻撃者はこの漏洩元の追跡が不可能なコンテンツ復号化鍵を用いてデジタルコンテンツの復号化を行う端末を作成し、コンテンツの不正利用を行うおそれがある。そのようなコンテンツ不正利用を防ぐ手段の一つとして、出力装置毎に個別の鍵を持たせることによって、漏洩元の出力装置の追跡を可能にするシステムが考えられる。全出力装置に同じデータを送るような放送局型のコンテンツ配信において、コンテンツ不正利用を防止する方式としては、例えば下記非特許文献1に記載されたコンテンツ配信システムがある。

【0004】

図34は、前記非特許文献1に記載された従来のコンテンツ配信システムを示すものである。図34において、通信路90は、後述する鍵発行センタ91及びサーバ92及び複数の出力装置93a～93nを接続している通信路であり、インターネット等のネットワークで実現されている。鍵発行センタ91は、コンテンツCNTの暗号化及び復号化を行うコンテンツ暗号化鍵CEK、コンテンツ復号化鍵CDKをそれぞれ作成し、コンテンツ暗号化鍵CEKをサーバ92に、コンテンツ復号化鍵CDKを鍵更新情報UPDKEY= $\text{Enc}(\text{IKa}, \text{CDK}) || \text{Enc}(\text{IKb}, \text{CDK}) || \dots || \text{Enc}(\text{IKn}, \text{CDK})$ として複数の出力装置93a～93nに配信する。ここで、 $\text{Enc}(\text{K}, \text{P})$ は暗号化鍵Kを用いて平文Pを暗号化した際の暗号文を意味する。また、 $\text{IKa} \dots \text{IKn}$ は、鍵発行センタ91と複数の出力装置93a～93nの全ての組に予め一つ与えられる個別鍵のことであり、例えば鍵発行センタ91と出力装置93aは個別鍵IKaを、鍵発行センタ91と出力装置93bは個別鍵IKbを、鍵発行センタ91と出力装置93nは個別鍵IKnを予め共有しているとする。サーバ92はコンテンツ暗号化鍵CEKを基にコンテンツCNTの暗号化を行い、暗号化されたコンテンツENCNTを複数の出力装置93a～93nに配信し、複数の出力装置93a～93nは鍵更新情報UPDKEYを基に受信した暗号化コンテンツENCNTの復号化を行い、その復号化コンテンツDECCNTを外部へ出力する。ここで、コンテンツ暗号化鍵CEK及びコンテンツ復号化鍵CDKは、全ての出力装置93a～93nにおいて共通の値である。そのため、ある個別鍵を取得した攻撃者が、漏洩元の追跡が不可能なコンテンツ復号化鍵CDKを埋め込んだ

不正な出力装置を作成する場合が考えられる。しかし、このようなコンテンツ復号化鍵CDKを埋め込んだ不正な出力装置は、鍵発行センタ91がコンテンツ暗号化鍵CEK及びコンテンツ復号化鍵CDKを新たな値に更新することで以後コンテンツを利用出来ないように無効化することができる。

#### 【0005】

ここでは、各構成要素の動作についてもう少し詳細に説明する。まず、全ての出力装置93a~93nでコンテンツ復号化鍵CDKを共有する方法について説明する。初めに、鍵発行センタ91は、コンテンツ暗号化鍵CEK及びコンテンツ復号化鍵CDKを生成し、そのコンテンツ暗号化鍵CEKをサーバ92へ送信する。そして、それぞれの出力装置93a~93nと予め共有している個別鍵IKa、IKb、...、IKnに基づき、そのコンテンツ復号化鍵CDKを暗号化し、その各暗号文Enc( IKa, CDK)、Enc( IKb, CDK)、...、Enc( IKn, CDK)を結合した値を鍵更新情報UPDKEY=Enc( IKa, CDK) || Enc( IKb, CDK) || ... Enc( IKn, CDK)として複数の出力装置93a~93nへ向けて配信する。サーバ92はコンテンツ暗号化鍵CEKを受信し、また、出力装置93aは、鍵更新情報UPDKEYを受信し、鍵更新情報UPDKEYの中から自身の持つ個別鍵IKaに対応する暗号文Enc( IKa, CDK)を抜き出し、個別鍵IKaに基づき暗号文Enc( IKa, CDK)の復号化を行い、コンテンツ復号化鍵CDKを取得する。なお、出力装置93a以外の出力装置93b~93nの場合も、出力装置93aと同様に、各々の出力装置が持つ個別鍵に対応する暗号文を鍵更新情報UPDKEYから抜き出し、その暗号文を復号化することで、コンテンツ復号化鍵CDKを取得する。こうすることによって、全出力装置93a~93nでコンテンツ復号化鍵CDKを共有することが出来る。

#### 【0006】

次に、コンテンツを配信する場合の動作について説明する。まず、サーバ92は、外部からコンテンツCNTを受け取り、コンテンツ暗号化鍵CEKに基づきそのコンテンツCNTの暗号化を行い、その暗号化コンテンツENCCNT=Enc( CEK, CNT)を複数の出力装置93a~93nへ向けて配信する。暗号化コンテンツENCCNTを受信した複数の出力装置93a~93nは、コンテンツ復号化鍵CDKに基づき暗号化コンテンツENCCNTの復号化を行い、その復号化コンテンツDECCNTを外部へ出力する。

。

#### 【0007】

なお、鍵発行センタ91はある特定の個別鍵を有する出力装置を無効化し、コンテンツCNTを復号化出来ないようにすることも出来る。ここでは、出力装置93aの個別鍵を有する出力機器を無効化する場合について説明する。まず、鍵発行センタ91は外部から、出力装置93aを識別する出力装置識別子AIDaを受け取り、コンテンツ暗号化鍵CEK及びコンテンツ復号化鍵CDKを新たに生成し、そのコンテンツ暗号化鍵CEKをサーバ92に送信する。その後、出力装置識別子AIDaに対応する出力装置93aと予め共有している個別鍵IKaを除く全ての個別鍵IKb~IKnを用いて、そのコンテンツ復号化鍵CDKの暗号化を行い、その各暗号文Enc( IKb, CDK)、...、Enc( IKn, CDK)を結合した値を鍵更新情報UPDKEY=Enc( IKb, CDK) || ... Enc( IKn, CDK)として複数の出力装置93a~93nへ配信する。そうすることにより、出力装置識別子AIDaに対応する出力装置93a以外の出力装置93b~93nではコンテンツ復号化鍵CDKを取得することが出来るため、暗号化コンテンツENCCNT=Enc( CDK, CNT)を正しく復号化出来るが、出力装置識別子AIDaに対応する出力装置93aではコンテンツ復号化鍵CDKを取得出来ないため、暗号化コンテンツENCCNT=Enc( CDK, CNT)を復号化出来なくすることが出来る。なお、出力装置93a以外の出力装置93b~93nを無効化する場合も、出力装置93aの場合と同様の動作となるが、コンテンツ復号化鍵CDKを暗号化するのに用いる個別鍵が変わる点異なる。このようにすることによって、鍵発行センタ91は、出力装置を無効化することも出来る。

## 【0008】

このようなシステムにより、もし攻撃者によって、出力装置 93a~93n のうちの何れかの出力装置に埋め込まれている個別鍵が不正に取得され、攻撃者がその個別鍵を用いた出力装置を作ったとしても、その出力装置に埋め込まれている個別鍵から漏洩元の出力装置を追跡することが出来るため、対象出力装置の無効化などの対策を打つことが可能となる。

【非特許文献 1】「デジタル放送局システムのしくみ」、映像情報メディア学会 編、オーム出版局

## 【発明の開示】

## 【発明が解決しようとする課題】

## 【0009】

しかしながら、先に述べた従来の構成では、コンテンツ復号化鍵を埋め込んだ不正な出力装置を無効化するために、鍵発行センタがコンテンツ暗号化鍵及び対応するコンテンツ復号化鍵を更新したときに、出力装置へ配信する鍵更新情報のデータサイズが出力装置の数に比例して大きくなるという課題を有していた。

本発明は、上記課題を解決するもので、コンテンツ復号化鍵を埋め込んだ不正な出力装置を無効化するために、鍵発行センタがコンテンツ暗号化鍵及び対応するコンテンツ復号化鍵を更新したときに、出力装置へ配信するデータサイズを削減することが可能なコンテンツ配信システムを提供することを目的とする。

## 【課題を解決するための手段】

## 【0010】

請求項 1 における発明は、コンテンツを配信するコンテンツ配信システムであって、前記コンテンツ配信システムは、前記コンテンツを暗号化して配信するサーバと、暗号化された前記コンテンツを受信、復号化する複数の出力装置と、から構成され、前記サーバと前記出力装置のそれぞれは通信路を介して通信可能であって、さらに、各出力装置は、所定の鍵割当方法により個別に割り当てられた割当ノード復号化鍵群を保持しており、前記鍵割当方法は、一以上の木構造を用いており、各々の前記木構造は複数のノードから構成され、前記複数のノードは複数の階層（第 0 階層から第  $n$  階層： $n$  は 1 以上の自然数）により分類され、ただし、前記第 0 階層は一つの前記ノードから構成され、前記木構造の全ての前記ノードに一以上のノード暗号化鍵及び対応するノード復号化鍵の組を設定し、前記第  $i$  階層（ $i$  は 1 から  $n$  までの自然数）の前記ノードは、前記第 0 階層から前記第  $i-1$  階層のいずれか一つの前記ノードである親ノードと線で結ばれており、前記第  $n$  階層の前記ノード、および、前記第  $j$  階層（ $j$  は 1 から  $n-1$  までの自然数）の前記ノードであり、前記第  $j+1$  階層から前記第  $n$  階層のいずれの前記ノードにも線で結ばれていない前記ノードを末端ノードとし、前記末端ノードに対して、関連ノード集合は、前記末端ノードと、前記末端ノードの親ノードと、前記関連ノード集合に属するノードの親ノードから成り、前記関連ノード集合に属するノードに設定された前記ノード復号化鍵を割当ノード復号化鍵群とし、ノード暗号化鍵群を、全ての前記ノードに設定された前記ノード暗号化鍵とし、前記出力装置に前記末端ノードのいずれかを対応づけ、前記末端ノードの前記関連ノード集合に対応する前記割当ノード復号化鍵群を割り当てる方法であり、前記サーバは、前記鍵割当方法により予め与えられる前記ノード暗号化鍵群を保持する鍵情報格納部と、前記ノード暗号化鍵群の中から一以上の前記ノード暗号化鍵を選定し選定ノード暗号化鍵群とし、前記選定ノード暗号化鍵群は、少なくとも前記末端ノードに設定されている前記ノード暗号化鍵を含み、かつ、前記末端ノード以外の前記ノードに設定されている前記ノード暗号化鍵を含み、前記選定ノード暗号化鍵群の中の前記ノード暗号化鍵の各々を用いて、予め与えられるコンテンツ復号化鍵を暗号化することによって、暗号化コンテンツ鍵群を生成するコンテンツ鍵選択部と、外部から前記コンテンツを受信する入力部と、前記コンテンツ復号化鍵に対応し予め与えられるコンテンツ暗号化鍵に基づき前記コンテンツを暗号化する暗号化部と、前記暗号化コンテンツ及び前記暗号化コンテンツ鍵群を前記出力装置に配信する送信部と、を備え、前記出力装置は、前記暗号化コンテンツ及び前

記暗号化コンテンツ鍵群を受信する第一受信部と、前記鍵割当方法により予め与えられる前記割当ノード復号化鍵群を保持するノード鍵格納部と、前記割当ノード復号化鍵群及び前記暗号化コンテンツ鍵群に基づき前記コンテンツ復号化鍵を取得する復号化鍵取得部と、前記コンテンツ復号化鍵に基づき前記暗号化コンテンツを復号化する第一復号化部と、を備えることを特徴とする。

#### 【0011】

請求項2における発明は、請求項1に記載のコンテンツ配信システムであって、前記サーバは、さらに、複数の前記コンテンツを受信するとし、外部から前記コンテンツを受信した際に、前回前記コンテンツを暗号化する際に用いた一以上の前記コンテンツ暗号化鍵及び対応する前記コンテンツ復号化鍵の組とは異なる一以上の前記コンテンツ暗号化鍵及び対応する前記コンテンツ復号化鍵の組を新たに生成するコンテンツ鍵生成部を備えることを特徴とする。

#### 【0012】

請求項3における発明は、請求項1または請求項2に記載のコンテンツ配信システムであって、前記サーバは、さらに、複数の前記コンテンツを受信するとし、前記コンテンツ鍵選択部は、さらに、前記サーバが外部から前記コンテンツを受信した際に、前回選定した前記末端ノードとは異なる前記末端ノードに設定されている前記ノード暗号化鍵を含む前記選定ノード暗号化鍵群を新たに作成することを特徴とする。

#### 【0013】

請求項4における発明は、請求項1から請求項3のいずれか1項に記載のコンテンツ配信システムであって、前記サーバは、さらに、前記割当ノード復号化鍵群における前記ノード暗号化鍵の鍵選定情報を複数保持する鍵選定情報格納部を備え、前記コンテンツ鍵選択部は、前記鍵選定情報格納部の保持している複数の前記鍵選定情報を基に、前記選定ノード暗号化鍵群を作成することを特徴とする。

#### 【0014】

請求項5における発明は、請求項1から請求項3のいずれか1項に記載のコンテンツ配信システムであって、前記サーバ及び前記出力装置は、さらに、前記選定ノード暗号化鍵群における前記ノード暗号化鍵の鍵選定情報と前記鍵選定情報を識別する鍵選定識別子を対応付けて複数保持している鍵選定情報格納部を備え、前記コンテンツ鍵選択部は、前記鍵選定情報格納部の保持している複数の前記鍵選定情報のいずれか1つの前記鍵選定情報を基に前記選定ノード暗号化鍵群を作成し、基にした前記鍵選定情報に対応する前記鍵選定識別子を前記送信部へ出力し、前記送信部は、前記暗号化コンテンツ及び前記暗号化コンテンツ鍵群及び前記鍵選定識別子を前記出力装置に配信し、前記第一受信部は、前記暗号化コンテンツ及び前記暗号化コンテンツ鍵群及び前記鍵選定識別子を受信し、前記復号化鍵取得部は、前記鍵選定情報格納部の保持している複数の前記鍵選定情報を用いて、前記割当ノード復号化鍵群及び前記暗号化コンテンツ鍵群及び前記鍵選定識別子を基に、前記コンテンツ復号化鍵を取得することを特徴とする。

#### 【0015】

請求項6における発明は、請求項4または請求項5に記載のコンテンツ配信システムであって、前記コンテンツ鍵選択部は、前記鍵選定情報格納部が保持している複数の前記鍵選定情報の中からランダムに一つの前記鍵選定情報を選択し、選択された前記鍵選定情報を基に前記選定ノード暗号化鍵群を作成することを特徴とする。

請求項7における発明は、請求項4または請求項5に記載のコンテンツ配信システムであって、前記コンテンツ鍵選択部は、前記鍵選定情報格納部が保持している複数の前記鍵選定情報の中の前記鍵選定情報を周期的に一つ選択し、選択された前記鍵選定情報を基に選定ノード暗号化鍵群を作成することを特徴とする。

#### 【0016】

請求項8における発明は、請求項1から請求項7のいずれか1項に記載のコンテンツ配信システムであって、前記鍵割当方法における本構造は、N分木（Nは2以上の自然数）であることを特徴とする。

請求項 9 における発明は、請求項 1 から請求項 8 のいずれか 1 項に記載のコンテンツ配信システムであって、前記コンテンツ配信システムは、さらに、前記通信路を介して前記出力装置のそれぞれとサーバに接続され、前記ノード暗号化鍵群及び複数の前記割当ノード復号化鍵群を配信する鍵発行センタを備え、前記鍵発行センタは、前記鍵割当方法に基づき、前記ノード暗号化鍵群及び複数の割当ノード復号化鍵群を生成するノード鍵生成部と、前記ノード暗号化鍵群を前記サーバに送信する第一送信部と、複数の前記割当ノード復号化鍵群と複数の前記出力装置の対応情報を保持する出力装置対応情報格納部と、前記対応情報に基づき複数の前記割当ノード復号化鍵群を前記それぞれの出力装置に配信する第二送信部と、を備え、前記サーバは、受信した前記ノード暗号化鍵群を前記鍵情報格納部に格納する受信部を備え、前記出力装置は、受信した前記割当ノード復号化鍵群を前記ノード鍵格納部へ格納する第二受信部を備えることを特徴とする。

#### 【0017】

請求項 10 における発明は、請求項 1 から請求項 8 のいずれか 1 項に記載のコンテンツ配信システムであって、前記コンテンツ配信システムは、さらに、前記通信路を介して前記出力装置のそれぞれとサーバに接続され、前記ノード暗号化鍵群及び鍵更新情報を配信する鍵発行センタを備え、前記鍵発行センタは、予め各々の前記出力装置に与えられる個別鍵を保持する出力装置対応情報格納部と、各々の前記出力装置に与えられる前記個別鍵を基に各々の前記出力装置に割り当てられた前記割当ノード復号化鍵群を暗号化し、鍵更新情報を生成する第一暗号化部と、前記鍵更新情報を前記出力装置へ配信する第二送信部とを備え、前記出力装置は、前記鍵更新情報を受信する第二受信部と、予め与えられる前記個別鍵を保持する個別鍵格納部と、前記個別鍵に基づき受信した前記鍵更新情報の復号化を行い、復号化された前記割当ノード復号化鍵群を前記ノード鍵格納部へ格納する第二復号化部と、を備えることを特徴とする。

#### 【0018】

請求項 11 における発明は、請求項 10 に記載のコンテンツ配信システムであって、前記出力装置対応情報格納部は、さらに、各々の前記出力装置に対応付けられている出力装置識別子と前記割当ノード復号化鍵群の対応情報を保持し、前記鍵発行センタは、外部から前記出力装置識別子を受信した場合に、前記出力装置識別子を基に、前記出力装置対応情報格納部の保持している前記対応情報を更新し、さらに、前記ノード鍵生成要求を前記ノード鍵生成部へ出力する対応情報更新部を備え、前記ノード鍵生成部は、前記ノード鍵生成要求を受信した場合に、前記鍵割当方法に基づき、前記ノード暗号化鍵群及び複数の割当ノード復号化鍵群を生成することを特徴とする。

#### 【0019】

請求項 12 における発明は、請求項 10 または請求項 11 に記載のコンテンツ配信システムであって、前記ノード鍵生成部は、前記鍵割当方法に基づき、前記ノード暗号化鍵群及び複数の割当ノード復号化鍵群を生成した場合、前記第一暗号化部へ鍵更新情報生成要求を出力し、前記第一暗号化部は、前記鍵更新情報生成要求を受信した場合、各々の前記出力装置に与えられる前記個別鍵を基に各々の前記出力装置に割り当てられた前記割当ノード復号化鍵群を暗号化し、鍵更新情報を生成することを特徴とする。

#### 【0020】

請求項 13 における発明は、コンテンツを暗号化して配信するサーバと、通信路を介して前記サーバに接続され、前記コンテンツを受信する出力装置と、を備えるコンテンツ配信システムにおける出力装置であって、さらに、各出力装置は、所定の鍵割当方法により個別に割り当てられた割当ノード復号化鍵群を保持しており、前記サーバ及び前記出力装置は、さらに、前記割当ノード復号化鍵群における前記ノード暗号化鍵の鍵選定情報と前記鍵選定情報を識別する鍵選定識別子に対応付けて複数保持している鍵選定情報格納部を備え、前記鍵割当方法は、一以上の木構造を用いており、各々の前記木構造は複数のノードから構成され、前記複数のノードは複数の階層（第 0 階層から第  $n$  階層： $n$  は 1 以上の自然数）により分類され、ただし、前記第 0 階層は一つの前記ノードから構成され、前記木構造の全ての前記ノードに一以上のノード暗号化鍵及び対応するノード復号化鍵の組を



設定し、前記第  $i$  階層 ( $i$  は 1 から  $n$  までの自然数) の前記ノードは、前記第 0 階層から前記第  $i-1$  階層のいずれか一つの前記ノードである親ノードと線で結ばれており、前記第  $n$  階層の前記ノード、および、前記第  $j$  階層 ( $j$  は 1 から  $n-1$  までの自然数) の前記ノードであり、前記第  $j+1$  階層から前記第  $n$  階層のいずれの前記ノードにも線で結ばれていない前記ノードを末端ノードとし、前記末端ノードに対して、関連ノード集合は、前記末端ノードと、前記末端ノードの親ノードと、前記関連ノード集合に属するノードの親ノードから成り、前記関連ノード集合に属するノードに設定された前記ノード復号化鍵を割当ノード復号化鍵群とし、ノード暗号化鍵群を、全ての前記ノードに設定された前記ノード暗号化鍵とし、前記出力装置に前記末端ノードのいずれかを対応づけ、前記末端ノードの前記関連ノード集合に対応する前記割当ノード復号化鍵群を割り当てる方法であり、前記出力装置は、外部から前記暗号化コンテンツ及び前記暗号化コンテンツ鍵群及び前記鍵選定識別子を受信する第一受信部と、前記鍵割当方法により予め与えられる前記割当ノード復号化鍵群を保持するノード鍵格納部と、前記鍵選定情報格納部の保持している複数の前記鍵選定情報を用いて、前記割当ノード復号化鍵群及び前記暗号化コンテンツ鍵群及び前記鍵選定情報識別子を基に、前記コンテンツ復号化鍵を取得する復号化鍵取得部と、前記コンテンツ復号化鍵に基づき前記暗号化コンテンツを復号化する第一復号化部と、を備えることを特徴とする。

#### 【0021】

請求項 14 における発明は、請求項 13 に記載の出力装置であって、前記鍵割当方法における木構造は、 $N$  分木 ( $N$  は 2 以上の自然数) であることを特徴とする。

請求項 15 における発明は、請求項 13 または請求項 14 に記載の出力装置であって、前記コンテンツ配信システムは、さらに、前記通信路を介して前記出力装置のそれぞれとサーバに接続され、前記ノード暗号化鍵群及び複数の前記割当ノード復号化鍵群を配信する鍵発行センタを備え、さらに、外部から受信した前記割当ノード復号化鍵群を前記ノード鍵格納部へ格納する第二受信部と、を備えることを特徴とする。

#### 【0022】

請求項 16 における発明は、請求項 13 または請求項 14 に記載のコンテンツ配信システムであって、前記コンテンツ配信システムは、さらに、前記通信路を介して前記出力装置のそれぞれとサーバに接続され、前記ノード暗号化鍵群及び鍵更新情報を配信する鍵発行センタを備え、さらに、外部から前記鍵更新情報を受信する第二受信部と、予め与えられる個別鍵を保持する個別鍵格納部と、前記個別鍵に基づき受信した前記鍵更新情報の復号化を行い、復号化された前記割当ノード復号化鍵群を前記ノード鍵格納部へ格納する第二復号化部と、を備えることを特徴とする。

#### 【0023】

請求項 17 における発明は、コンテンツを暗号化して配信するサーバと、通信路を介して前記サーバに接続され、前記コンテンツを受信する処理をコンピュータに実行させるプログラムであって、所定の鍵割当方法により個別に割り当てられた割当ノード復号化鍵群を保持しており、さらに、前記割当ノード復号化鍵群における複数の前記ノード暗号化鍵の鍵選定情報と前記鍵選定情報を識別する鍵選定識別子の対応情報を保持しており、前記鍵割当方法は、一以上の木構造を用いており、各々の前記木構造は複数のノードから構成され、前記複数のノードは複数の階層 (第 0 階層から第  $n$  階層:  $n$  は 1 以上の自然数) により分類され、ただし、前記第 0 階層は一つの前記ノードから構成され、前記木構造の全ての前記ノードに一以上のノード暗号化鍵及び対応するノード復号化鍵の組を設定し、前記第  $i$  階層 ( $i$  は 1 から  $n$  までの自然数) の前記ノードは、前記第 0 階層から前記第  $i-1$  階層のいずれか一つの前記ノードである親ノードと線で結ばれており、前記第  $n$  階層の前記ノード、および、前記第  $j$  階層 ( $j$  は 1 から  $n-1$  までの自然数) の前記ノードであり、前記第  $j+1$  階層から前記第  $n$  階層のいずれの前記ノードにも線で結ばれていない前記ノードを末端ノードとし、前記末端ノードに対して、関連ノード集合は、前記末端ノードと、前記末端ノードの親ノードと、前記関連ノード集合に属するノードの親ノードから成り、前記関連ノード集合に属するノードに設定された前記ノード復号化鍵を割当ノード

復号化鍵群とし、ノード暗号化鍵群を、全ての前記ノードに設定された前記ノード暗号化鍵とし、前記出力装置に前記末端ノードのいずれかを対応づけ、前記末端ノードの前記関連ノード集合に対応する前記割当ノード復号化鍵群を割り当てる方法であり、外部から前記暗号化コンテンツ及び前記暗号化コンテンツ鍵群及び前記鍵選定識別子を受信するステップと、複数の前記鍵選定情報を用いて、前記割当ノード復号化鍵群及び前記暗号化コンテンツ鍵群及び前記鍵選定情報識別子を基に、前記コンテンツ復号化鍵を取得するステップと、前記コンテンツ復号化鍵に基づき前記暗号化コンテンツを復号化するステップと、をコンピュータに実行させることを特徴とする。

**【0024】**

請求項18における発明は、請求項17に記載のプログラムを媒体に記録することを特長とする。

請求項19における発明は、請求項17に記載のプログラムであって、さらに、前記鍵割当方法における木構造は、N分木（Nは2以上の自然数）であることを特徴とする。

請求項20における発明は、請求項19に記載のプログラムを媒体に記録することを特徴とする。

**【0025】**

請求項21における発明は、請求項17または請求項19に記載のプログラムであって、さらに、前記通信路を介して前記プログラムと前記サーバに接続され、前記ノード暗号化鍵群及び複数の前記割当ノード復号化鍵群を配信する鍵発行センタを備え、さらに、外部から前記割当ノード復号化鍵群を受信するステップと、をコンピュータに実行させることを特徴とする。

**【0026】**

請求項22における発明は、請求項21に記載のプログラムを媒体に記録することを特徴とする。

請求項23における発明は、請求項17または請求項19に記載のプログラムであって、さらに、前記通信路を介して前記プログラムと前記サーバに接続され、前記ノード暗号化鍵群及び鍵更新情報を配信する鍵発行センタを備え、さらに、外部から前記鍵更新情報を受信するステップと、予め与えられる個別鍵に基づき受信した前記鍵更新情報の復号化を行うステップと、をコンピュータに実行させることを特徴とする。

**【0027】**

請求項24における発明は、請求項23に記載のプログラムを記録した媒体。

請求項25における発明は、コンテンツを配信するコンテンツ配信方法であって、前記コンテンツ配信方法は、所定の鍵割当方法を基に予め与えられたノード暗号化鍵群を用いて前記コンテンツを暗号化して配信するコンテンツ配信ステップと、前記鍵割当方法を基に予め与えられた割当ノード復号化鍵群を用いて暗号化された前記コンテンツを復号化するコンテンツ受信ステップと、から構成され、前記鍵割当方法は、一以上の木構造を用いており、各々の前記木構造は複数のノードから構成され、前記複数のノードは複数の階層（第0階層から第n階層：nは1以上の自然数）により分類され、ただし、前記第0階層は一つの前記ノードから構成され、前記木構造の全ての前記ノードに一以上のノード暗号化鍵及び対応するノード復号化鍵の組を設定し、前記第i階層（iは1からnまでの自然数）の前記ノードは、前記第0階層から前記第i-1階層のいずれか一つの前記ノードである親ノードと線で結ばれており、前記第n階層の前記ノード、および、前記第j階層（jは1からn-1までの自然数）の前記ノードであり、前記第j+1階層から前記第n階層のいずれの前記ノードにも線で結ばれていない前記ノードを末端ノードとし、前記末端ノードに対して、関連ノード集合は、前記末端ノードと、前記末端ノードの親ノードと、前記関連ノード集合に属するノードの親ノードから成り、前記関連ノード集合に属するノードに設定された前記ノード復号化鍵を割当ノード復号化鍵群とし、ノード暗号化鍵群を、全ての前記ノードに設定された前記ノード暗号化鍵とし、前記コンテンツ受信ステップに前記末端ノードのいずれかを対応づけ、前記末端ノードの前記関連ノード集合に対応する前記割当ノード復号化鍵群を割り当てる方法であり、前記コンテンツ配信ステップは、

前記鍵割当方法により予め与えられる前記ノード暗号化鍵群の中から一以上の前記ノード暗号化鍵を選定し選定ノード暗号化鍵群とし、前記選定ノード暗号化鍵群は、少なくとも前記末端ノードに設定されている前記ノード暗号化鍵を含み、かつ、前記末端ノード以外の前記ノードに設定されている前記ノード暗号化鍵を含み、前記選定ノード暗号化鍵群の中の前記ノード暗号化鍵の各々を用いて、予め与えられるコンテンツ復号化鍵を暗号化することによって、暗号化コンテンツ鍵群を生成するステップと、外部から前記コンテンツを受信するステップと、前記コンテンツ復号化鍵に対応し予め与えられるコンテンツ暗号化鍵に基づき前記コンテンツを暗号化するステップと、前記暗号化コンテンツ及び前記暗号化コンテンツ鍵群を前記出力装置に配信するステップと、を含み、前記コンテンツ受信ステップは、前記暗号化コンテンツ及び前記暗号化コンテンツ鍵群を受信するステップと、前記鍵割当方法により予め与えられる前記割当ノード復号化鍵群及び前記暗号化コンテンツ鍵群に基づき前記コンテンツ復号化鍵を取得するステップと、前記コンテンツ復号化鍵に基づき前記暗号化コンテンツを復号化するステップと、を含むことを特徴とする。

#### 【発明の効果】

##### 【0028】

本発明のコンテンツ配信システムによれば、漏洩元の追跡が出来ない全出力装置共通のコンテンツ復号化鍵を埋め込んだ不正な出力装置をすばやく無効化することを目的に、鍵発行センタがコンテンツ暗号化鍵及び対応するコンテンツ復号化鍵を更新したときに、出力装置へ配信するデータサイズの削減を行った。このことによって、限られたデータサイズしか転送出来ない通信路においても、より多くコンテンツ暗号化鍵及びコンテンツ復号化鍵を更新することが出来るため、漏洩元の追跡が不可能なコンテンツ復号化鍵を埋め込んだ不正な出力装置を作成する攻撃に対する耐性が増すことになる。

#### 【発明を実施するための最良の形態】

##### 【0029】

以下本発明に係るコンテンツ配信システムの実施の形態について、図面を参照しながら説明する。

##### （実施の形態1）

本発明に係る一つの実施の形態としてのコンテンツ配信システム1について説明する。最初に、図1を用いて本実施の形態の概要を説明する。なお、以後、コンテンツを出力する出力装置が8台の場合について説明を行うが、これは8台以外であっても同様に実現可能である。

##### 【0030】

図1において、10は後述する鍵発行センタ11と後述するサーバ12と後述する8台の出力装置13a～13hとが接続されている通信路であり、インターネット等のネットワークである。ここで、鍵発行センタ11と出力装置13a～13hの全ての組には、予め各々の組が共有している一つの個別鍵が与えられているとし、例えば鍵発行センタ11と出力装置13aは個別鍵IKaを、鍵発行センタ11と出力装置13bは個別鍵IKbを、鍵発行センタ11と出力装置13hは個別鍵IKhを予め共有しているとする。

##### 【0031】

ここでは、各構成要素の動作について説明する。まず、全ての出力装置13a～13hがコンテンツ復号化鍵を取得する際に用いるノード暗号化鍵及びノード復号化鍵に関する情報を配布する方法について説明する。

鍵発行センタ11は事前準備として、まず、例えば図2で示すような一つのノードが2つの子ノードを持つ2分木で深さが3の木構造を1つ用意し、サーバ12と共有しておく。なお、本発明で使用する木構造はN分木（Nは3以上の自然数）であっても、深さがM（Mは2以上の自然数）であっても良く、複数の木構造を利用しても良い。これ以降、本発明で使用する木構造において、ルートノードの深さ（階層）を第0階層、ルートノード（第0階層）の子ノードの深さを第1階層、その第1階層のノードの子ノードの深さを第2階層、その第2階層のノードの子ノードの深さを第3階層と呼ぶ。そして、全ノードの名前付けとして、ルートノードを第0ノード、第0ノードの2つの子ノードのうち1つを



第1ノード、もう一方を第2ノードとする。また、第1ノードの2つの子ノードを第3ノードと第4ノードとし、第2ノードの2つの子ノードを第5ノードと第6ノードとする。さらに、第3ノードの2つの子ノードを第7ノードと第8ノードとし、第4ノードの2つの子ノードを第9ノードと第10ノードとし、第5ノードの2つの子ノードを第11ノードと第12ノードとし、第6ノードの2つの子ノードを第13ノードと第14ノードとする。つまり、今回使用する木構造は全部で15個のノードから構成される。そして第0ノードには第0ノード暗号化鍵NEK0と対応する第0ノード復号化鍵NDK0のペアを、第1ノードには第1ノード暗号化鍵NEK1と対応する第1ノード復号化鍵NDK1のペアを、・・・、第14ノードには第14ノード暗号化鍵NEK14及び対応する第14ノード復号化鍵NDK14のペアをそれぞれランダムに作成し、設定する。ここで、各々の第0ノード復号化鍵NDK0から第14ノード復号化鍵NDK14は、各々の第0ノード暗号化鍵NEK0から第14ノード暗号化鍵NEK14に対応する復号化鍵であるとし、また、第0ノード復号化鍵NDK0から第14ノード復号化鍵NDK14のそれぞれは各々異なる値になるように設定する。そして第0ノード暗号化鍵NEK0から第14ノード暗号化鍵NEK14により構成される図3で示すような暗号化ノード鍵群ALLNEK=NEK0||NEK1||・・・||NEK14をサーバ12へ送信する。また次に、各出力装置13a～13hを、第3階層の各ノードである末端ノードのそれぞれに一つずつ対応付ける。なお、末端ノードには、複数の出力装置を対応付けても良い。そして、各出力装置13a～13hには、末端ノードからルートノードまで辿っていった時に通過する計4つのノード復号化鍵を割り当てる。例えば図2のような木構造の場合、出力装置13aには、第0ノード復号化鍵NDK0と第1ノード復号化鍵NDK1と第3ノード復号化鍵NDK3と第7ノード復号化鍵NDK7を、出力装置13fには、第0ノード復号化鍵NDK0と第2ノード復号化鍵NDK2と第5ノード復号化鍵NDK5と第12ノード復号化鍵NDK12を割り当てる。そして、各出力装置13a～13hそれぞれに割り当てられた4つのノード復号化鍵を連結したものを、各々の出力装置と予め共有している個別鍵IKa～IKhを用いて暗号化する。例えば、出力装置13aに対しては、暗号文Enc (IKa、NDK0||NDK1||NDK3||NDK7)、出力装置13fに対しては、暗号文Enc (IKf、NDK0||NDK2||NDK5||NDK12)となる。そして、各々の暗号文を連結したものを鍵更新情報UPDKEY=Enc (IKa、NDK0||NDK1||NDK3||NDK7)||・・・||Enc (IKh、NDK0||NDK2||NDK6||NDK14)として、複数の出力装置13a～13hへ配信する。

#### 【0032】

次に、サーバ12がコンテンツ復号化鍵CDKを出力装置13a～13hへ配信する場合の動作について説明する。サーバ12は、まず、コンテンツCNTを暗号化、復号化するのに用いるコンテンツ暗号化鍵CEK、対応するコンテンツ復号化鍵CDKをランダムに生成する。次に、そのコンテンツ復号化鍵CDKを暗号化する際に用いる複数のノード暗号化鍵を以下のような方法でノード暗号化鍵群の中から選定する。まず、木構造の末端ノードに対応付けられているノード暗号化鍵 (NEK7～NEK14) を一つランダムに選定する。ここでは、コンテンツ暗号化鍵CEK、コンテンツ復号化鍵CDKを更新する毎に選定する末端ノード (第7ノード～第14ノード) を変更する点に注意する。そして、選定したノード暗号化鍵に対応するノード復号化鍵が割り当てられていない出力装置13a～13hが保有しているノード復号化鍵に対応するノード暗号化鍵を選定することを繰り返す。なお、選定済みのノード暗号化鍵に対応するノード復号化鍵が割り当てられていない出力装置13a～13hが存在しなくなるまで繰り返しても良い。上記のような方法により、ノード暗号化鍵群からコンテンツ復号化鍵CDKを暗号化する際に用いる複数のノード暗号化鍵を選定する。例えば、出力装置13aは第7ノード復号化鍵NDK7を、出力装置13bは第8ノード復号化鍵NDK8を、出力装置13c～13dは第4ノード復号化鍵NDK4を、出力装置13e～13hは第2ノード復号化鍵NDK2をそれぞれ保持しているので、第2ノード暗号化鍵NEK2と第4ノード暗号化鍵NEK4と第7

ノード暗号化鍵NEK7と第8ノード暗号化鍵NEK8を選定することはできる。そして、その選定された複数のノード暗号化鍵の各々を用いて、コンテンツ復号化鍵CDKを暗号化する。例えば、先ほどの例において各暗号文はEnc (NEK2, CDK)、Enc (NEK4, CDK)、Enc (NEK7, CDK)、Enc (NEK8, CDK)となる。そして、それら暗号化されたコンテンツ復号化鍵CDKから構成される暗号化コンテンツ鍵群ENCCKGを出力装置13a~13hへ送信する。例えば、先ほどの例においては、暗号化コンテンツ鍵群ENCCKG=Enc (NEK2, CDK) || Enc (NEK4, CDK) || Enc (NEK7, CDK) || Enc (NEK8, CDK)となる。出力装置13a~13hは、受信した暗号化コンテンツ鍵群ENCCKGから、自身が保有している割当ノード復号化鍵群の中のいずれかのノード復号化鍵に対応している暗号文を探し、その暗号文の復号化を行うことによってコンテンツ復号化鍵CDKを取得する。例えば、図2のような木構造の場合、出力装置13aは第7ノード復号化鍵NDK7を保有しているので、第7ノード暗号化鍵NEK7を基にしたコンテンツ復号化鍵CDKの暗号文Enc (NEK7, CDK)を復号化して、コンテンツ復号化鍵CDKを取得する。

#### 【0033】

ここで、サーバ12はコンテンツ暗号化鍵CEK、及び対応するコンテンツ復号化鍵CDKは更新することを想定し、また、そのコンテンツ復号化鍵CDKを暗号化する際に用いるノード暗号化鍵群の中から選定する複数のノード暗号化鍵も更新するようにする。

次に、サーバ12がコンテンツを出力装置13a~13hへ配信する場合の動作について説明する。サーバ12は、コンテンツ暗号化鍵CEKに基づいてコンテンツCNTの暗号化を行い、その暗号化コンテンツENCNT=Enc (CEK, CNT)を複数の出力装置13a~13hへ向けて配信する。出力装置13a~13hは、暗号化コンテンツENCNTを受信し、コンテンツ復号化鍵CDKに基づいて、暗号化コンテンツENCNTの復号化を行い、その復号化コンテンツDECNTを外へ出力する。

#### 【0034】

なお、本実施の形態であるコンテンツ配信システム1では、鍵発行センタ11がある特定の個別鍵を持つ出力装置を無効化し、コンテンツCNTを復号化出来ないようにすることも可能となる。これは以下のようにして実現可能である。ここでは、出力装置13aを無効化する場合について説明する。鍵発行センタ11は、外部から出力装置13aを識別する出力装置識別子AIDaを受け取り、全てのノード暗号化鍵及びノード暗号化鍵を新たに生成する。そして、全てのノード暗号化鍵 (NEK0~NEK14) から成る暗号化ノード鍵群ALLNEKをサーバ12へ送信する。また、出力装置13a以外の各出力装置13b~13hに個別に全てのノード復号化鍵 (NDK0~NDK14) から4つのノード復号化鍵を割り当て、割り当てられた4つのノード復号化鍵から構成される割当ノード復号化鍵群 (ANDKGb~ANDKGh) を作成する。そして、出力装置識別子AIDaに対応する出力装置13a以外のそれぞれの出力装置13b~13hが持つ個別鍵IKb~IKhに基づいて、それぞれの割当ノード復号化鍵群ANDKGb~ANDKGhの暗号化を行う。そしてその暗号文を連結した値を暗号化コンテンツ鍵群ENCCKGとして複数の出力装置13a~13hへ向けて配信する。そうすることにより、その鍵発行センタ11に入力された出力装置識別子AIDaに対応する出力装置13aでは、暗号化コンテンツ鍵ENCCKGの中に個別鍵IKaに対応する割当ノード復号化鍵群の暗号文がないので、新たに4つのノード復号化鍵を取得出来なくなり、その結果コンテンツ復号化鍵CDKを生成出来なくなる。つまり、暗号化コンテンツENCNT=Enc (CDK, CNT)を復号化出来なくなるので、その出力装置13aの無効化を実現出来る。なお、出力装置13a以外の出力装置13b~13hを無効化する場合も、出力装置13aと同様の動作を行うが、持っている個別鍵は出力装置毎に異なるため、割当ノード復号化鍵の各々を暗号化する個別鍵が違う点異なる。以上のようにして、鍵発行センタ11はある特定の個別鍵を有する出力装置の無効化が実現することが出来る。

#### 【0035】

以上が、本実施の形態の概要である。以下に、本発明のコンテンツ配信システムの一実施形態であるコンテンツ配信システム 1 の詳細について説明を行う。これらの構成要素について詳細に説明する。

#### <コンテンツ配信システム 1 の構成>

コンテンツ配信システム 1 は、図 1 に示すように、通信路 10 と、鍵発行センタ 11 と、サーバ 12 と、複数の出力装置 13a～13h から構成される。

#### 【0036】

鍵発行センタ 11 はコンテンツ復号化鍵 CDK を暗号化するのに用いるノード暗号化鍵群 ALLNEK をサーバ 12 へ送信する。また、コンテンツ復号化鍵 CDK を取得する際に用いるノード復号化鍵 (NDK0～NDK14) のいずれか 4 つを、図 2 で示すような木構造を用いて、各々の出力装置 13a～13h に個別に割り当てる。そして、その各出力装置 13a～13h に割り当てられたそれぞれ 4 つのノード復号化鍵を連結したものを各出力装置の持つ個別鍵 IKa～IKh を用いて暗号化する。その暗号文を結合した値を鍵更新情報 UPDKY として複数の出力装置 13a～13h へ配信する。出力装置 13a～13h は、鍵更新情報 UPDKY の中から、自身が持つ個別鍵 IKa～IKh に対応する暗号文を取得し、その暗号文を個別鍵を用いて復号化することによって、自身の出力装置に割り当てられた 4 つのノード復号化鍵を取得する。サーバ 12 は、コンテンツ CNT を暗号化、復号化するコンテンツ暗号化鍵 CEK、コンテンツ復号化鍵 CDK を作成し、そのコンテンツ復号化鍵 CDK を暗号化する際に用いる複数のノード暗号化鍵を以下のような方法でノード暗号化鍵群の中から選定する。まず、木構造の末端ノードに対応付けられているノード暗号化鍵 (NEK7～NEK14) を一つランダムに選定する。ここでは、コンテンツ暗号化鍵 CEK、コンテンツ復号化鍵 CDK を更新する毎に選定する末端ノード (第 7 ノード～第 14 ノード) を変更する点に注意する。そして、選定したノード暗号化鍵に対応するノード復号化鍵が割り当てられていない出力装置 13a～13h が保有しているノード復号化鍵に対応するノード暗号化鍵を選定することを繰り返す。上記のような方法により、ノード暗号化鍵群からコンテンツ復号化鍵 CDK を暗号化する際に用いる複数のノード暗号化鍵を選定する。そして、その選定された複数のノード暗号化鍵それぞれを用いて、コンテンツ復号化鍵 CDK の暗号化を行い、その暗号文を連結したものを暗号化コンテンツ鍵群 ENCCDKG として出力装置 13a～13h へ送信する。そして、出力装置 13a～13h は、自身の保有する割当ノード復号化鍵の中の 4 つのノード復号化鍵のいずれかを用いて、暗号化コンテンツ鍵群 ENCCDKG の中の対応するコンテンツ復号化鍵の暗号文を復号化して、コンテンツ復号化鍵 CDK を取得する。サーバ 12 はコンテンツ CNT を暗号化して暗号化コンテンツ ENCCNT = Enc (CEK, CNT) として出力装置 13a～13h へ配信し、出力装置 13a～13h はコンテンツ復号化鍵 CDK に基づき、受信した暗号化コンテンツ ENCCNT の復号化を行い、その復号化コンテンツ DECCNT を外部へ出力する。

#### 【0037】

以下に、これらの構成要素について詳細に説明する。まず、通信路 10 の構成について述べ、続いて鍵発行センタ 11 及びサーバ 12 及び複数の出力装置 13a～13h の構成と動作について図を用いて説明する。

#### <通信路 10 の構成>

通信路は、例えば、インターネット、電話回線や専用線等のようなネットワークである。

#### 【0038】

#### <鍵発行センタ 11 の構成>

鍵発行センタ 11 は、図 4 に示すように、ノード鍵生成部 111、第一送信部 112、出力装置対応情報格納部 113、第一暗号化部 114、第二送信部 115、入力部 116、対応情報更新部 117 から構成される。

#### (1) ノード鍵生成部 111

ノード鍵生成部 111 は、予めノード鍵更新条件が与えられており、そのノード鍵更新

条件を満たした場合、もしくは、後述する対応情報更新部117からノード鍵生成要求REQ1を受信した場合、もしくは、鍵発行センタ11が動作を開始した場合、ノード鍵生成部111は、まず第0ノード暗号化鍵NEK0と対応する第0ノード復号化鍵NDK0のペア、第1ノード暗号化鍵NEK1と対応する第1ノード復号化鍵NDK1のペア、・・・、第14ノード暗号化鍵NEK14と対応する第14ノード復号化鍵NDK14のペアの計15ペアをそれぞれランダムに作成する。ここで、各ノード暗号化鍵及びノード復号化鍵は、例えばAES暗号方式の128ビット鍵などである。そして、各ノード暗号化鍵(NEK0～NEK14)を連結したものから構成される図3で示すようなノード暗号化鍵群ALLNEK=NEK0||NEK1||・・・||NEK14を作成し、そのノード暗号化鍵群ALLNEKを第一送信部112に出力する。次に、例えば、図2のような木構造の場合、8つの末端ノード(第7ノード～第14ノード)の各ノードに出力装置13a～13hをそれぞれ対応付け、そして、各出力装置13a～13hに対応付けられた末端ノードからルートノードに辿っていった時に通過する4つのノード復号化鍵を割り当てる。例えば、図2のような木構造の場合、出力装置13aには、第0ノード復号化鍵NDK0と第1ノード復号化鍵NDK1と第3ノード復号化鍵NDK3と第7ノード復号化鍵NDK7を割り当て、出力装置13fには、第0ノード復号化鍵NDK0と第2ノードNDK2と第5ノード復号化鍵NDK5と第12ノード復号化鍵NDK12を割り当てる。そして、各出力装置13a～13hのそれぞれに割り当てられた4つのノード復号化鍵から構成される割当ノード復号化鍵群ANDKGa～ANDKGhを作成する。例えば、図5が示すように出力装置13a向けの割当ノード復号化鍵群はANDKGa=NDK0||NDK1||NDK3||NDK7であり、出力装置13f向けの割当ノード復号化鍵群はANDKGf=NDK0||NDK2||NDK5||NDK12である。そして、その生成した割当ノード復号化鍵群ANDKGa～ANDKGhのそれぞれを各々の出力装置識別子AIDa～AIDhに対応付けて、図6で示すような出力装置対応情報格納部113へ格納する。そして最後に、鍵更新情報生成要求REQ2を第一暗号化部114へ出力する。なお、ノード鍵生成部111に予め与えられるノード鍵更新条件は、例えば、“1年毎”などであり、これはノード鍵生成部111がカウンタを保持することで実現出来る。

#### 【0039】

##### (2) 第一送信部112

第一送信部112は、ノード鍵生成部111から受け取ったノード暗号化鍵群ALLNEKを通信路10を経由してサーバ12に送信するものである。

##### (3) 出力装置対応情報格納部113

出力装置対応情報格納部113は、図6で示すように、出力装置13a～13hを識別する複数の出力装置識別子AIDa～AIDhと、その各出力装置13a～13hに予め与えられている複数の個別鍵IKa～IKh及び割当ノード復号化鍵群ANDKGa～ANDKGhを保持するものである。例えば、図6においては、出力装置識別子AIDaに対応づけられている出力装置13aは個別鍵IKaと割当ノード復号化鍵群ANDKGaを保持し、出力装置識別子AIDbに対応づけられている出力装置13bは個別鍵IKb及び割当ノード復号化鍵群ANDKGbを保持し、出力装置識別子AIDhに対応づけられている出力装置13hは個別鍵IKh及び割当ノード復号化鍵群ANDKGhを保持していることを表している。出力装置情報格納部113へは、ノード鍵生成部111及び第一暗号化部114及び対応情報更新部117からアクセス可能である。

#### 【0040】

##### (4) 第一暗号化部114

第一暗号化部114は、ノード鍵生成部111から鍵更新情報生成要求REQ2を受け取った場合、出力装置対応情報格納部113にアクセスして、複数の出力装置識別子AIDa～AIDh及び個別鍵IKa～IKh及び割当ノード復号化鍵群ANDKGa～ANDKGhを全て取得する。そして、まず、出力装置識別子AIDaに対して、対応している個別鍵IKaに基づいて割当ノード復号化鍵群ANDKGaの暗号化を行い、その暗号

文を暗号化割当ノード復号化鍵群  $ENCANDKG_a = Enc(IK_a, ANDKG_a)$  として、出力装置識別子  $AID_a$  に対応付ける。続いて、他の出力装置識別子  $AID_b \sim AID_h$  に対しても、同様に、対応づけられている個別鍵に基づいて対応付けられている割当ノード復号化鍵群の暗号化を行い、その暗号文  $Enc(IK_b, ANDKG_b)$ 、 $\dots$ 、 $Enc(IK_n, ANDKG_h)$  を暗号化割当ノード復号化鍵群  $ENCANDKG_b$ 、 $\dots$ 、 $ENCANDKG_h$  とし、それぞれの出力装置識別子  $AID_b \sim AID_h$  に対応付ける。そして、図7で示すような、複数の出力装置識別子  $AID_a \sim AID_h$  及び暗号化割当ノード復号化鍵群  $ENCANDKG_a \sim ENCANDKG_h$  から構成される鍵更新情報  $UPDKEY = \{AID_a, ENCANDKG_a\} \parallel \{AID_b, ENCANDKG_b\} \dots \parallel \{AID_h, ENCANDKG_h\}$  を生成し、その鍵更新情報  $UPDKEY$  を第二送信部 115 に出力する。ここで割当ノード復号化鍵群を暗号化するのに使用する暗号化アルゴリズムは、例えば、ブロック暗号の AES 方式や DES 方式などであり、各出力装置 13a $\sim$ 13h のそれぞれの第二復号化部 138a で用いる復号化アルゴリズムと同じ方式を用いる。

#### 【0041】

##### (5) 第二送信部 115

第二送信部 115 は、第一暗号化部 114 から鍵更新情報  $UPDKEY$  を受信した場合、受信した鍵更新情報  $UPDKEY$  を通信路 10 を経由して複数の出力装置 13a $\sim$ 13h に配信する。

##### (6) 入力部 116

入力部 116 は、外部から出力装置 13a $\sim$ 13h のいずれかを識別する出力装置識別子  $AID_a \sim AID_h$  のいずれかを入力出来るものであり、外部から出力装置識別子  $AID_a \sim AID_h$  のいずれかを受信した場合、対応情報更新部 117 にその受信した出力装置識別子を出力する。なお、入力部 116 は、鍵発行センタ 11 がある特定の個別鍵を有する出力装置の無効化を行う際に、どの出力装置を無効化するかを判別するために利用するものなので、鍵発行センタ 11 が出力装置の無効化を行わない場合は、入力部 116 が鍵発行センタ 11 の中に存在していなくても良い。

#### 【0042】

##### (7) 対応情報更新部 117

対応情報更新部 117 は、入力部 116 から出力装置識別子  $AID_a \sim AID_h$  のいずれかを受信した場合、まず図6で示すような出力装置対応情報格納部 113 にアクセスし、その中から受信した出力装置識別子及びその出力装置識別子に対応付けられている個別鍵及び割当ノード復号化鍵群を出力装置対応情報格納部 113 から削除する。例えば、図6のような出力装置対応情報格納部 113 において、対応情報更新部 117 が出力装置識別子  $AID_a$  を受信したとすると、対応する出力装置識別子  $AID_a$  及び個別鍵  $IK_a$  及び割当ノード復号化鍵群  $ANDKG_a$  を出力装置対応情報格納部 113 から削除することで、図8のようになる。削除が終わったら、ノード鍵生成部 111 にノード鍵生成要求  $REQ_1$  を出力する。なお、対応情報更新部 117 は、鍵発行センタ 11 がある特定の個別鍵を有する出力装置の無効化を行う際に利用するものであるため、鍵発行センタ 11 が出力装置の無効化を行わない場合は、対応情報更新部 117 が鍵発行センタ 11 の中に存在していなくても良い。

#### 【0043】

##### <鍵発行センタ 11 の動作>

以上で、鍵発行センタ 11 の構成について説明を行ったが、ここでは鍵発行センタ 11 の動作について説明する。まず、予め与えられるノード鍵更新条件を満たした場合、もしくは、鍵発行センタ 11 が動作を開始した場合などにおいて、複数のノード暗号化鍵及びノード復号化鍵を更新する場合の動作について図9に示すフローチャートを用いて説明する。また、鍵発行センタ 11 は入力部 116 及び対応情報更新部 117 も構成要素とすることによって、ある特定の個別鍵を有する出力装置を無効化する機能を持たせることも可能であるが、ここでは具体例として、出力装置 13a を無効化する時の動作について図1

0に示すフローチャートを用いて説明する。

【0044】

《ノード暗号化鍵及びノード復号化鍵の更新時の動作》

ノード鍵生成部111は、第0ノード暗号化鍵NEK0と対応する第0ノード復号化鍵NDK0、・・・、第14ノード暗号化鍵NEK14と対応する第14ノード復号化鍵NDK14の計15ペアをランダムに作成する(S1101)。

ノード鍵生成部111は、図3で示すような、第0ノード暗号化鍵NEK0から第14ノード暗号化鍵NEK14の計15個のノード暗号化鍵から構成されるノード暗号化鍵群ALLNEKを作成する(S1102)。

【0045】

ノード鍵生成部111は、ノード暗号化鍵群ALLNEKを、第一送信部112へ出力する(S1103)。

第一送信部112は、受信したノード暗号化鍵群ALLNEKを、サーバ12へ向けて送信する(S1104)。

ノード鍵生成部111は、出力装置対応情報格納部113に格納されている割当ノード復号化鍵群ANDKga～ANDKghを全て削除する。また、図2で示すような予め与えられる木構造に対して、8つの末端ノードの各ノードに出力装置13a～13hを一つずつそれぞれ対応付ける(S1105)。

【0046】

ノード鍵生成部111は、まだ割当ノード復号化鍵群を生成していない出力装置に対して、対応付けられている末端ノードからルートノードまで辿っていった時に通過する4つのノード復号化鍵から構成される割当ノード復号化鍵群を作成する。そして、その割当ノード復号化鍵群を出力装置識別子に対応づけて、出力装置対応情報格納部113へ格納する(S1106)。

【0047】

もし、出力装置対応情報格納部113の中にある全ての出力装置識別子AIDa～AIDhに対して割当ノード復号化鍵群ANDKga～ANDKghを割り当てられたら、ステップS1108へ進む。もし、残っていたらステップS1106に戻る(S1107)。

ノード鍵生成部111は、鍵更新情報生成要求REQ2を第一暗号化部114へ出力する(S1108)。

【0048】

鍵更新情報生成要求REQ2を受け取った第一暗号化部114は、出力装置対応情報格納部113にアクセスして、出力装置識別子AIDa～AIDh及び個別鍵IKa～IKh及び割当ノード復号化鍵群ANDKga～ANDKghをそれぞれ全て取得する(S1109)。

暗号化部115は、各々の個別鍵IKa～IKhに基づいて、各々の割当ノード復号化鍵群ANDKga～ANDKghを暗号化し、その暗号化された割当ノード復号化鍵群ENCANDKga～ENCANDKgh及び暗号化に用いた個別鍵IKa～IKhに対応する出力装置識別子AIDa～AIDhのそれぞれから構成される鍵更新情報UPDKEYを生成する(S1110)。

【0049】

第一暗号化部114は、生成した鍵更新情報UPDKEYを第二送信部115へ出力する(S1111)。

第二送信部115は、鍵更新情報UPDKEYを受け取り、その受信した鍵更新情報UPDKEYを複数の出力装置13a～13hへ向けて配信し、終了する(S1112)。

《出力装置13aの無効化時の動作》

入力部116は、受信した出力装置識別子AIDaを、対応情報更新部117へ出力する(S1151)。

【0050】



対応情報更新部 117 は、入力部 116 から受信した出力装置識別子 A I D a 及びその出力装置識別子 A I D a に対応する個別鍵 I K a と割当ノード復号化鍵群 A N D K G a を出力装置対応情報格納部 113 から削除する (S 1152)。

対応情報更新部 117 は、ノード鍵生成部 111 へノード鍵生成要求 R E Q 1 を出力し、ステップ S 1101 に進む (S 1153)。

#### 【0051】

なお、出力装置 13 a 以外の出力装置 13 b ~ 13 h のいずれかを無効化する時の動作も、出力装置 13 a の場合とほぼ同様の動作となるが、対応情報更新部 117 において、出力装置対応情報格納部 113 から削除する出力装置識別子及び個別鍵及び割当ノード復号化鍵群が無効化する出力装置 13 b ~ 13 h に依存して変化する点異なる。

以上が、コンテンツ配信システム 1 の構成要素である鍵発行センタ 11 の構成と動作である。続いて、サーバ 12 の構成と動作について説明を行う。

#### 【0052】

##### <サーバ 12 の構成>

サーバ 12 は、図 10 に示すように、入力部 121、暗号化部 122、鍵情報格納部 123、コンテンツ鍵選択部 124、送信部 125、受信部 126、コンテンツ鍵生成部 127 から構成される。

##### (1) 入力部 121

入力部 121 は、外部からコンテンツ C N T を入力できるものである。外部から入力されるコンテンツ C N T は、複数の出力装置 13 a ~ 13 h で出力可能なフォーマット形式であって、例えば、M P E G フォーマットによる動画データや M P 3 フォーマットによる音声データなどである。入力部 121 は、外部からコンテンツ C N T を受信した場合、その受信したコンテンツ C N T を暗号化部 122 に出力する。

#### 【0053】

##### (2) 暗号化部 122

暗号化部 122 は、入力部 121 からコンテンツ C N T を受信した場合、図 12 に示すような鍵情報格納部 123 にアクセスして、コンテンツ暗号化鍵 C E K を取得し、取得したコンテンツ暗号化鍵 C E K に基づいて、逐次、入力部 121 から受け取ったコンテンツ C N T の暗号化を行う。ここでコンテンツ C N T の暗号化に使用する暗号アルゴリズムは、例えば、ブロック暗号の A E S 方式や D E S 方式などであり、後述する複数の出力装置 13 a ~ 13 h のそれぞれの第一復号化部 135 において暗号化コンテンツ E N C C N T を復号化するのに用いるアルゴリズムと同じ方式を用いる。その後、暗号化されたコンテンツ E N C C N T をコンテンツ鍵選択部 124 に出力する。

#### 【0054】

##### (3) 鍵情報格納部 123

鍵情報格納部 123 は、図 12 で示すように、コンテンツ暗号化鍵 C E K 及びコンテンツ復号化鍵 C D K 及びノード暗号化鍵群 A L L N E K 及びノード復号化鍵群 A L L N D K が格納されている。

##### (4) コンテンツ鍵選択部 124

コンテンツ鍵選択部 124 は、暗号化部 122 から暗号化コンテンツ E N C C N T を受信した場合、鍵情報格納部 123 にアクセスして、コンテンツ復号化鍵 C D K 及びノード暗号化鍵群 A L L N E K を取得する。そして、そのコンテンツ復号化鍵 C D K を暗号化する際に用いるノード暗号化鍵群 A L L N E K の中の複数のノード暗号化鍵 (N E K 0 ~ N E K 14) を以下のような方法で選定する。まず、木構造の末端ノードに対応付けられているノード暗号化鍵 (N E K 7 ~ N E K 14) を一つランダムに選定する。ここでは、コンテンツ暗号化鍵 C E K、コンテンツ復号化鍵 C D K を更新する毎に選定する末端ノード (第 7 ノード ~ 第 14 ノード) を変更する点に注意する。そして、選定したノード暗号化鍵に対応するノード復号化鍵が割り当てられていない出力装置 13 a ~ 13 h が保有しているノード復号化鍵に対応するノード暗号化鍵を選定することを繰り返す。上記のような方法により、ノード暗号化鍵群からコンテンツ復号化鍵 C D K を暗号化する際に用いる複

数のノード暗号化鍵を選定する。そして、その選定された複数のノード暗号化鍵それぞれを用いて、コンテンツ復号化鍵CDKの暗号化を行う。例えば、出力装置13aは第7ノード復号化鍵NDK7を、出力装置13bは第8ノード復号化鍵NDK8を、出力装置13c~13dは第4ノード復号化鍵NDK4を、出力装置13e~13hは第2ノード復号化鍵NDK2をそれぞれ保持しているので、暗号化第2ノード復号化鍵ENCNDK2=Enc(NDK2, CDK)と暗号化第4ノード復号化鍵ENCNDK4=Enc(NDK4, CDK)と暗号化第7ノード復号化鍵ENCNDK7=Enc(NDK7, CDK)と暗号化第8ノード復号化鍵ENCNDK8=Enc(NDK8, CDK)は選定可能である。そして、それら複数の暗号化ノード復号化鍵から成る図14で示すような暗号化コンテンツ鍵群ENCCDKGを生成し、受信した暗号化コンテンツENCNTとその暗号化コンテンツ鍵群ENCCDKGを送信部125へ出力する。例えば、複数のノード暗号化鍵としてNEK2とNEK4とNEK7とNEK8を選定した場合、ENCCDKG=Enc(NEK2, CDK) || Enc(NEK4, CDK) || Enc(NEK7, CDK) || Enc(NEK8, CDK)となる。

#### 【0055】

##### (5) 送信部125

送信部125は、逐次、コンテンツ鍵選択部124から受け取った暗号化コンテンツENCNT及び暗号化コンテンツ鍵群ENCCDKGを、通信路10を経由して複数の出力装置13a~13hに配信する。

##### (6) 受信部126

受信部126が、鍵発行センタ11からノード暗号化鍵群ALLNEKを受信した場合、受信したノード暗号化鍵群ALLNEKを鍵情報格納部123に格納する。

#### 【0056】

##### (7) コンテンツ鍵生成部127

コンテンツ鍵生成部127には、予めコンテンツ鍵更新条件が与えられており、その条件を満たした場合に、コンテンツ暗号化鍵CEK及び対応するコンテンツ復号化鍵CDKのペアをランダムに生成する。例えば、コンテンツ暗号化鍵CEK及びコンテンツ復号化鍵CDKはAES方式の128ビット鍵である。そして、コンテンツ暗号化鍵CEK及びコンテンツ復号化鍵CDKを鍵情報格納部123へ格納する。なお、コンテンツ鍵生成部127に予め与えられるコンテンツ鍵更新条件は、例えば、“1分毎”などであり、これはコンテンツ鍵生成部127がカウンタを保持することで実現出来る。

#### 【0057】

##### <サーバ12の動作>

以上で、サーバ12の構成について説明を行ったが、ここでサーバ12の動作について説明する。まず、コンテンツ配信時の動作について図15に示すフローチャートを用いて説明する。そして、ノード暗号化鍵群ALLNEKを受信する場合の動作について図16に示すフローチャートを用いて説明する。最後に、コンテンツ暗号化鍵CEK、コンテンツ復号化鍵CDKを更新する時の動作について図17に示すフローチャートを用いて説明する。

#### 【0058】

##### <コンテンツCNTの配信時の動作>

受信部121が、外部からコンテンツCNTを受け取った場合、ステップS1202に進む。受信していない場合、終了する(S1201)。

受信部121は、受信したコンテンツCNTを暗号化部122に出力する(S1202)。

#### 【0059】

コンテンツCNTを受信した第一暗号化部122は、鍵情報格納部113にアクセスして、コンテンツ暗号化鍵CEKを取得する(S1203)。

第一暗号化部122は、コンテンツ暗号化鍵CEKに基づいてコンテンツCNTの暗号化を行い、その暗号化コンテンツENCNTをコンテンツ鍵選択部124へ出力する(



S1204)。

【0060】

暗号化コンテンツ ENCCNT を受け取ったコンテンツ鍵選択部 124 は、鍵情報格納部 123 にアクセスして、ノード暗号化群 ALLNEK 及びコンテンツ復号化鍵 CDK を取得する (S1205)。

コンテンツ鍵選択部 124 は、木構造の末端ノードに対応付けられているノード暗号化鍵 (NEK7~NEK14) を一つランダムに選定し、そして、選定したノード暗号化鍵に対応するノード復号化鍵が割り当てられていない出力装置 13a~13h が保有しているノード復号化鍵に対応するノード暗号化鍵を選定することを繰り返す。上記のような方法により、ノード暗号化鍵群からコンテンツ復号化鍵 CDK を暗号化する際に用いる複数のノード暗号化鍵を選定し、その選定された複数のノード暗号化鍵それぞれを用いて、コンテンツ復号化鍵 CDK の暗号化を行う。そして、それら複数の暗号文から構成される暗号化コンテンツ鍵群 ENCCDKG を生成する (S1206)。

【0061】

コンテンツ鍵選択部 124 は、暗号化コンテンツ鍵群 ENCCDKG と暗号化コンテンツ ENCCNT を、送信部 125 へ出力する (S1207)。

暗号化コンテンツ ENCCNT 及び暗号化コンテンツ鍵群 ENCCDK を受け取った受信部 125 は、その暗号化コンテンツ ENCCNT 及び暗号化コンテンツ鍵群 ENCCDK を出力装置 13a~13h へ向けて配信し、終了する (S1208)。

【0062】

＜ノード暗号化鍵群受信時の動作＞

受信部 126 が、鍵発行センタ 11 からノード暗号化鍵群 ALLNEK を受け取った場合、ステップ S1232 に進む。受信していない場合、終了する (S1231)。

受信部 126 は、受信したノード暗号化鍵群 ALLNEK を鍵情報格納部 123 へ格納する。終了する (S1232)。

【0063】

＜コンテンツ暗号化鍵、コンテンツ復号化鍵更新時の動作＞

コンテンツ鍵生成部 127 は、予め与えられたコンテンツ鍵更新条件を満たしている場合、ステップ S1262 に進む。コンテンツ鍵更新条件を満たしていない場合、終了する (S1261)。

コンテンツ鍵生成部 127 は、コンテンツ暗号化鍵 CEK 及び対応するコンテンツ復号化鍵 CDK のペアをランダムに生成する (S1262)。

【0064】

コンテンツ鍵生成部 127 は、コンテンツ暗号化鍵 CEK 及びコンテンツ復号化鍵 CDK を鍵情報格納部 123 へ格納し、終了する (S1263)。

以上が、コンテンツ配信システム 1 の構成要素であるサーバ 12 の構成と動作である。続いて、出力装置 13a~13h の構成と動作について説明を行う。まず、出力装置 13a の構成と動作について説明を行い、次に、出力装置 13a と他の出力装置 13b~13h と異なる点について述べる。

【0065】

＜出力装置 13a の構成＞

出力装置 13a は、図 18 に示すように、第一受信部 131、復号化鍵取得部 132a、ノード鍵格納部 133a、第一復号化部 134、出力部 135、第二受信部 136、第二復号化部 137a、個別鍵格納部 138a から構成される。ここで、第一受信部 131、第一復号化部 134、出力部 135、第二受信部 136 は出力装置 13a~13h において共通の構成要素であり、復号化鍵取得部 132a、ノード鍵格納部 133a、第二復号化部 137a、個別鍵格納部 138a は、出力装置 13a 固有の構成要素である。

【0066】

(1) 第一受信部 131

第一受信部 131 が、サーバ 12 から暗号化コンテンツ ENCCNT 及び暗号化コンテ

ンツ鍵群ENCCKGを受信した場合、受信した暗号化コンテンツ鍵群ENCCKGを復号化鍵取得部132aに出力し、その後、暗号化コンテンツENCNTを第一復号化部134に出力する。

【0067】

(2) 復号化鍵生成部132a

復号化鍵生成部132aが、第一受信部131から暗号化コンテンツ鍵群ENCCKGを受信した場合、まず、図19で示すようなノード鍵格納部133aにアクセスし、割当ノード復号化鍵群ANDKGaを取得する。そして、割当ノード復号化鍵群ANDKGaを構成している4つのノード復号化鍵を取得する。例えば、図5のような割当ノード復号化鍵群ANDKGaの場合、第0ノード復号化鍵NDK0と第1ノード復号化鍵NDK1と第3ノード復号化鍵NDK3と第7ノード復号化鍵NDK7を取得することになる。その後、受信した暗号化コンテンツ鍵群ENCCKGの中から、割当ノード復号化鍵群ANDKGaに含まれていた4つのノード復号化鍵のいずれかに対応する暗号文を探索する。例えば、図14のような暗号化コンテンツ鍵群ENCCKGの場合、暗号化第7ノード復号化鍵ENCNDK7=Enc(NDK7, CDK)となる。そして、割当ノード復号化鍵群ANDKGaに含まれていた4つのいずれかのノード復号化鍵を用いて、対応する暗号化ノード復号化鍵を復号化することによって、コンテンツ復号化鍵CDKを取得する。その後、コンテンツ復号化鍵CDKを第一復号化部134へ出力する。

【0068】

(3) ノード鍵格納部133a

ノード鍵格納部133aは、図19で示すように、割当ノード復号化鍵群ANDKGaを保持するものである。このノード鍵格納部133aへは、復号化鍵生成部132a及び第二復号化部137aからアクセス可能である。

(4) 第一復号化部134

第一復号化部134は、第一受信部131から暗号化コンテンツENCNTを受信し、復号化鍵取得部132aからコンテンツ復号化鍵CDKを受信した場合、そのコンテンツ復号化鍵CDKに基づいて暗号化コンテンツENCNTの復号化を行う。ここで復号化に使用するアルゴリズムは、例えば、ブロック暗号のAES方式やDES方式などであり、サーバ12の暗号化部122で用いるアルゴリズムと同じ方式を用いる。復号化した復号化コンテンツDECCNT=Dec(CDK, ENCNT)を出力部135へ出力する。ここで、Dec(K, C)は復号化鍵Kをもとに、暗号文Cを復号化した際の復号文とする。

【0069】

(5) 出力部135

出力部135は、第一復号化部134から復号化コンテンツDECCNTを受信した場合、受信した復号化コンテンツDECCNTを外部へ出力する。

(6) 第二受信部136

第二受信部136が、サーバ12から鍵更新情報UPDKYを受信した場合、受信した鍵更新情報UPDKYを第二復号化部137aに出力する。

【0070】

(7) 第二復号化部137a

第二復号化部137aは、第二受信部136から鍵更新情報UPDKYを受信した場合、まず図20に示すような個別鍵格納部138aから出力装置識別子AIDa及び個別鍵IKaを取得する。そして、受信した鍵更新情報UPDKYの中から、個別鍵格納部138aに格納されていた出力装置識別子AIDaに対応する暗号化割当ノード復号化鍵群ENCANDKGaを探索する。そして、個別鍵格納部138aに格納されていた個別鍵IKaに基づいて、その対応する暗号化割当ノード復号化鍵群ENCANDKGaの復号化を行い、その復号化した割当ノード復号化鍵群ANKaをノード鍵格納部133aに格納する。

【0071】

## (8) 個別鍵格納部 138a

個別鍵格納部 138a は、図 20 で示すように、出力装置識別子 A I D a 及び個別鍵 I K a を保持するものである。この個別鍵格納部 138a へは、第二復号化部 137a からアクセス可能である。

## &lt;出力装置 13a の動作&gt;

以上で、出力装置 13a の構成について説明を行ったが、ここで出力装置 13a の動作について説明する。まず、暗号化されたコンテンツ E N C C N T を受信した場合の動作について図 21 に示すフローチャートを用いて説明する。そして、鍵更新情報 U P D K E Y を受信した際の動作について図 22 に示すフローチャートを用いて説明する。

## 【0072】

## &lt;暗号化コンテンツ受信時の動作&gt;

第一受信部 131 が、暗号化コンテンツ E N C C N T 及び暗号化コンテンツ鍵群 E N C C D K G を受け取った場合、ステップ S 1302 に進む。受信していない場合、終了する (S 1301)。

第一受信部 131 は、受信した暗号化コンテンツ鍵群 E N C C D K G を復号化鍵取得部 132a に出力する (S 1302)。

## 【0073】

暗号化コンテンツ鍵群 E N C C D K G を受信した復号化鍵取得部 132a は、ノード鍵格納部 133a にアクセスして、割当ノード復号化鍵群 A N D K G a を取得する (S 1303)。

復号化鍵取得部 132a は、割当ノード復号化鍵群 A N D K G a から 4 つのノード復号化鍵を取得する。そして、暗号化コンテンツ鍵群 E N C C D K G の中において、その 4 つのノード復号化鍵のいずれかに対応づけられている暗号化ノード復号化鍵を探索し、その暗号化ノード復号化鍵に対応する 4 つのいずれかのノード復号化鍵を用いて復号化することによって、コンテンツ復号化鍵 C D K を取得する (S 1304)。

## 【0074】

復号化鍵生成部 132a は、コンテンツ復号化鍵 C D K を第一復号化部 134 へ出力する (S 1305)。

第一復号化部 134 は、受信したコンテンツ復号化鍵 C D K を基に、暗号化コンテンツ E N C C N T の復号化を行い、復号化コンテンツ D E C C N T を取得する (S 1306)。

。

## 【0075】

第一復号化部 134 は、復号化コンテンツ D E C C N T を、出力部 135 へ出力する (S 1307)。

出力部 135 は、第一復号化部 134 から復号化コンテンツ D E C C N T を受信し、受信した復号化コンテンツ D E C C N T を外部へ出力する。終了する (S 1308)。

## &lt;鍵更新情報 U P D K E Y の受信時の動作&gt;

第二受信部 136 が鍵更新情報 U P D K E Y を受信した場合、ステップ S 1352 に進む。受信していない場合、終了する (S 1351)。

## 【0076】

第二受信部 136 は、受信した鍵更新情報 U P D K E Y を第二復号化部 137a に出力する (S 1352)。

第二復号化部 137a は、個別鍵格納部 138a から出力装置識別子 A I D a 及び個別鍵 I K a を取得する (S 1353)。

第二復号化部 137a は、受信した鍵更新情報 U P D K E Y の中から、出力装置識別子 A I D a に対応する暗号化割当ノード復号化鍵群 E N C A N D K G a を取得する (S 1354)。

## 【0077】

第二復号化部 137a は、個別鍵 I K a に基づいて、暗号化割当ノード復号化鍵群 E N C A N D K G a の復号化を行い、割当ノード復号化鍵群 A N D K G a を取得する (S 1355)。

55)。

第二復号化部 137a は、割当ノード復号化鍵群 ANDKGa をノード鍵格納部 133a に格納し、終了する (S1356)。

#### 【0078】

以上が、コンテンツ配信システム 1 の構成要素である出力装置 13a の構成と動作である。なお、出力装置 13a と他のいずれの出力装置 13b ~ 13h とで異なる部分については、ノード鍵格納部 133a において出力装置 13a ~ 13h 毎に異なる割当ノード復号化鍵群 ANKa ~ ANKh が格納されている点と、個別鍵格納部 138a において出力装置 13a ~ 13h 毎に異なる出力装置識別子 AIDa ~ n 及び個別鍵 IKa ~ IKh が格納されている点と、復号化鍵取得生成部 132a において出力装置 13a ~ 13h 毎に異なる割当ノード復号化鍵群 ANKa ~ ANKh を用いる点と、第二復号化部 137a において出力装置 13a ~ 13h 毎に異なる個別鍵 IKa ~ IKh を用いる点異なる。

#### 【0079】

##### <実施の形態 1 の動作検証>

本実施の形態 1 において、それぞれの出力装置 13a ~ 13h には各々異なる割当ノード復号化鍵群 ANDKGa ~ ANDKGh が割り当てられているにもかかわらず、全出力装置 13a ~ 13h において同じコンテンツ復号化鍵 CDK が導出出来る理由について説明する。サーバ 12 は、ノード暗号化鍵群の中から各出力装置 13a ~ 13h が必ず保持しているノード復号化鍵から成る複数のノード復号化鍵に対応するノード暗号化鍵を選択して、その複数のノード暗号化鍵群を基にコンテンツ復号化鍵 CDK を暗号化している。そのため、出力装置 13a ~ 13h では同じコンテンツ復号化鍵 CDK が導出出来る。

#### 【0080】

実際に運用する場合には、例えば、図 28 から図 33 で示すようなコンテンツ復号化鍵を暗号化するのに用いる複数のノード暗号化鍵を、周期的に変更する。そうすることによって、出力装置では必ず末端 (第 3 階層) のノード復号化鍵を使用しないと、周期のある一定期間ではコンテンツ復号化鍵を得られないように出来る。また、もし末端のノード復号化鍵を埋め込んだ不正な出力装置が出回ったとしても、その末端のノード復号化鍵を調査することで、どの出力装置の個別鍵が漏洩したのか特定することが出来る。

#### 【0081】

##### <実施の形態 1 の効果>

本発明の実施の形態 1 によって、コンテンツ復号化鍵を埋め込んだ不正な出力装置を無効化するために、鍵発行センタがコンテンツ暗号化鍵及び対応するコンテンツ復号化鍵のペアを更新したときに、出力装置へ配信するデータサイズを削減できるようになった。具体的には、例えば、8 台の出力装置を想定する場合、従来例においてコンテンツ暗号化鍵 CEK 及び対応するコンテンツ復号化鍵 CDK のペアを更新するには、コンテンツ復号化鍵をそれぞれの個別鍵を用いて暗号化した際の暗号文として計 8 個が必要であった。しかし、本実施の形態においてコンテンツ暗号化鍵 CEK 及び対応するコンテンツ復号化鍵 CDK のペアを更新するには、例えば、図 28 から図 32 のような複数のノード暗号化鍵の割り当てを考えた場合、コンテンツ復号化鍵をそれぞれ 4 つのノード暗号化鍵を用いて暗号化した際の暗号文として計 4 個となり、データサイズの削減が実現出来る。このことによって、本実施の形態では、コンテンツ暗号化鍵及び対応するコンテンツ復号化鍵のペアをより多くの回数更新することが出来るようになるため、漏洩元の追跡が不可能なコンテンツ復号化鍵を埋め込んだ不正な出力装置を作成する攻撃に対する耐性を増すことが出来た。

#### 【0082】

##### <変形例>

上記に説明した実施の形態は、本発明の実施の一例であり、本発明はこの実施の形態に何ら限定されるものではなく、その旨を逸脱しない範囲において主な態様で実施し得るものである。以下のような場合も本発明に含まれる。

(1) 通信路 10 は、地上波又は衛星等の放送網であっても良い。

## 【0083】

(2) 出力装置 13a~13h の数は 8 台でなくても良い。これは、鍵の割り当てを決める木構造の深さを変更する等によって容易に実現可能である。

(3) 本実施の形態では、各末端ノードに一台の出力装置を設定していたが、一つの末端に複数の出力装置を設定しても良い。

(4) ノード暗号化鍵及び対応するノード復号化鍵が同一の値であっても良い。これにより、鍵情報格納部 123 は、ノード暗号化鍵群及びノード復号化鍵群のどちらかを格納するだけで十分となる。これは、コンテンツ鍵選択部 124 及び復号化鍵取得部 132a において共通鍵暗号などを用いれば実現可能である。

## 【0084】

(5) コンテンツ暗号化鍵 CEK 及び対応するコンテンツ復号化鍵 CDK が同一の値であっても良い。これにより、鍵情報格納部 123 は、コンテンツ暗号化鍵及びコンテンツ復号化鍵のどちらかを格納するだけで十分となる。これは、暗号化部 122 及び復号化部 134 において共通鍵暗号などを用いれば実現可能である。

(6) 鍵の割り当てを決める木構造は、図 2 のような形に限定されるものではない。例えば、図 23 で示すように 2 つの木構造を利用しても良いし、図 24 で示すように 4 つの木構造を利用しても良いし、それ以上の数の木構造を利用しても良い。また、図 25 のように、図 2 の木構造から第 2 階層の全てのノードをなくしたようなものでも良く、さらに、図 26 のように、図 2 の木構造から第 1 階層と第 2 階層の全てのノードをなくしたのも良い。

## 【0085】

(7) 鍵の割り当てを決める木構造に関して、図 2 では 1 つのノードが 2 つの子ノードを持つ 2 分木であったが、M 分木 (M は 3 以上の自然数) でも良い。例えば、図 27 で示すような 3 分木であっても良い。さらに、階層毎に、分木数が異なっても良い。

(8) 出力装置の無効化を行う機能を、鍵発行センタ 11 ではなくサーバ 12 が持つようにしても良い。つまり、サーバ 12 が出力装置識別子 AIDa~AIDh のいずれかを受信し、その出力装置識別子 AIDa~AIDh のいずれかを基に、鍵更新情報 UPDK EY を複数の出力装置 13a~13h に配信するようにしても良い。

## 【0086】

(9) 鍵発行センタ 11 のノード鍵生成部 111 は、外部からノード鍵生成要求情報 REQ1 を受信するようにして、そのノード鍵生成要求情報 REQ1 に基づき、複数のノード暗号化鍵及び対応するノード復号化鍵のペアを生成するようにしても良い。

(10) サーバ 12 のコンテンツ鍵生成部 127 は、外部からコンテンツ鍵生成要求情報 REQ3 を受信するようにして、そのコンテンツ鍵生成要求情報 REQ3 に基づき、コンテンツ暗号化鍵 CEK 及び対応するコンテンツ復号化鍵 CDK のペアを生成するようにしても良い。

## 【0087】

(11) サーバ 12 の送信部 125 は、前回送信した暗号化コンテンツ鍵群 ENCCDKG から変更がない場合は、暗号化コンテンツ ENCCNT だけを出力装置 13a~13h に送信するようにして、暗号化コンテンツ ENCCNT だけを受信した出力装置 13a~13h は、前回生成したコンテンツ復号化鍵 CDK を基に、暗号化コンテンツ ENCCNT を復号化するようにしても良い。

## 【0088】

(12) コンテンツ復号化鍵を暗号化する際に用いる複数のノード暗号化鍵の選択方法に関して、各出力装置 13a~13h が必ず 1 つずつ持つノード復号化鍵に対応するノード暗号化鍵を選択しなくてもよい。例えば、いくつかの出力装置が 2 つ以上持っているノード復号化鍵に対応するノード暗号化鍵を選択しても良いし、いくつかの出力装置が 1 つも持っていないノード復号化鍵に対応するノード暗号化鍵を選択しても良い。

## 【0089】

(13) コンテンツ復号化鍵 CDK を暗号化するのに用いるノード暗号化鍵群をパター

ン化して、サーバ12及び出力装置13a～13hで共有するようにしても良い。例えば、図28のようなノード暗号化鍵群パターンを第1パターンP1、図29のようなノード暗号化鍵群パターンを第2パターンP2、図30のようなノード暗号化鍵群パターンを第3パターンP3、図31のようなノード暗号化鍵群パターンを第4パターンP4とし、また、暗号化コンテンツ鍵群ENCCKGの中に第1パターンP1から第4パターンP4のいずれかを含むようにして、また、各出力装置13a～13hには、各ノード暗号化鍵群パターンとノード復号化鍵に関する対応情報を保持しており、復号化鍵取得部132aはその対応情報を基に、コンテンツ復号化鍵CDKを取得するようにしても良い。

#### 【0090】

(14) 末端ノードを除く各々のノードに対して、複数のノード暗号化鍵及び対応するノード復号化鍵を設定しても良い。

#### 【産業上の利用可能性】

#### 【0091】

本発明にかかるコンテンツ配信システムは、出力装置に埋め込まれている鍵が漏洩し、その鍵を用いて不正な出力装置が作成されたとしても、コンテンツ提供者はその不正な出力装置に埋め込まれている鍵情報を調査することによってその漏洩元を追跡出来るという効果を有し、インターネット等の通信路を用いてコンテンツを配信する際に有用である。また放送等の用途にも応用できる。

#### 【図面の簡単な説明】

#### 【0092】

【図1】 本発明の実施の形態1におけるコンテンツ配信システム1の概要図

【図2】 出力装置13a～13hに対するノード暗号化鍵及びノード復号化鍵の設定方法の一例

【図3】 本発明の実施の形態1におけるノード暗号化鍵群ALLNEKの一例を示す図

【図4】 本発明の実施の形態1における鍵発行センタ11の構成例を示す図

【図5】 本発明の実施の形態1における割当ノード復号化鍵群ANKaの一例を示す図

【図6】 本発明の実施の形態1における出力装置対応情報格納部113の構成例を示す図

【図7】 本発明の実施の形態1における鍵更新情報UPDKEYの一例を示す図

【図8】 本発明の実施の形態1における出力装置13aを無効化した後の出力装置対応情報格納部113の構成例を示す図

【図9】 本発明の実施の形態1における鍵発行センタ11のノード暗号化鍵、ノード復号化鍵配信時の処理の流れ図

【図10】 本発明の実施の形態1における鍵発行センタ11の出力装置13a無効化時の処理の流れ図

【図11】 本発明の実施の形態1におけるサーバ12の構成例を示す図

【図12】 本発明の実施の形態1における鍵情報格納部123の構成例を示す図

【図13】 本発明の実施の形態1におけるノード復号化鍵群ALLNDKの構成例を示す図

【図14】 本発明の実施の形態1における暗号化コンテンツ鍵群ENCCKGの一例を示す図

【図15】 本発明の実施の形態1におけるサーバ12のコンテンツ配信時の処理の流れ図

【図16】 本発明の実施の形態1におけるサーバ12のノード暗号化鍵群受信時の処理の流れ図

【図17】 本発明の実施の形態1におけるサーバ12のコンテンツ鍵更新時の処理の流れ図

【図18】 本発明の実施の形態1における出力装置13aの構成例を示す図

【図 19】 本発明の実施の形態 1 におけるノード鍵格納部 133a の構成例を示す図  
【図 20】 本発明の実施の形態 1 における個別鍵格納部 138a の構成例を示す図  
【図 21】 本発明の実施の形態 1 におけるサーバ 12 の暗号化コンテンツ受信時の処理の流れ図

【図 22】 本発明の実施の形態 1 におけるサーバ 12 の鍵更新情報受信時の処理の流れ図

【図 23】 出力装置 13a ~ 13h に対するノード暗号化鍵及びノード復号化鍵の割り当て方法の別の一例

【図 24】 出力装置 13a ~ 13h に対するノード暗号化鍵及びノード復号化鍵の割り当て方法の別の一例

【図 25】 出力装置 13a ~ 13h に対するノード暗号化鍵及びノード復号化鍵の割り当て方法の別の一例

【図 26】 出力装置 13a ~ 13h に対するノード暗号化鍵及びノード復号化鍵の割り当て方法の別の一例

【図 27】 出力装置 13a ~ 13i に対するノード暗号化鍵及びノード復号化鍵の割り当て方法の別の一例

【図 28】 コンテンツ復号化鍵を暗号化するのに用いる複数のノード暗号化鍵の選定例

【図 29】 コンテンツ復号化鍵を暗号化するのに用いる複数のノード暗号化鍵の選定例

【図 30】 コンテンツ復号化鍵を暗号化するのに用いる複数のノード暗号化鍵の選定例

【図 31】 コンテンツ復号化鍵を暗号化するのに用いる複数のノード暗号化鍵の選定例

【図 32】 コンテンツ復号化鍵を暗号化するのに用いる複数のノード暗号化鍵の選定例

【図 33】 コンテンツ復号化鍵を暗号化するのに用いる複数のノード暗号化鍵の選定例

【図 34】 従来のコンテンツ配信システムの概要図

【符号の説明】

【0093】

- 10 通信路
- 11 鍵発行センタ
- 12 サーバ
- 13a ~ 13h 出力装置
- 111 ノード鍵生成部
- 112 第一送信部
- 113 出力装置対応情報格納部
- 114 第一暗号化部
- 115 第二送信部
- 116、121 入力部
- 117 対応情報更新部
- 122 暗号化部
- 123 鍵情報格納部
- 124 コンテンツ鍵選択部
- 125 送信部
- 126 受信部
- 127 暗号化コンテンツ鍵生成部
- 131 第一受信部
- 132a 復号化鍵取得部

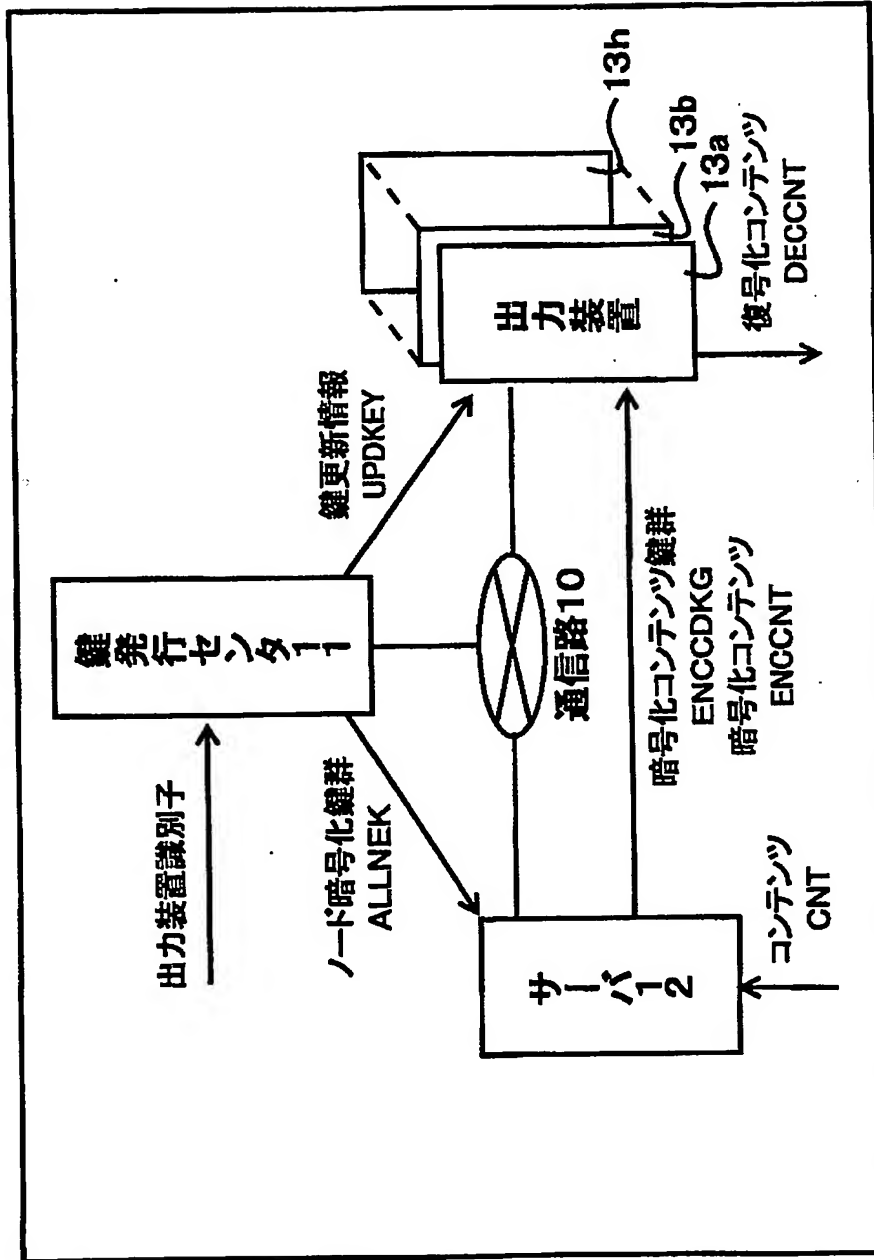
- 1 3 3 a ノード鍵格納部
- 1 3 4 第一復号化部
- 1 3 5 出力部
- 1 3 6 第二受信部
- 1 3 7 a 第二復号化部
- 1 3 8 a 個別鍵格納部



【書類名】 図面

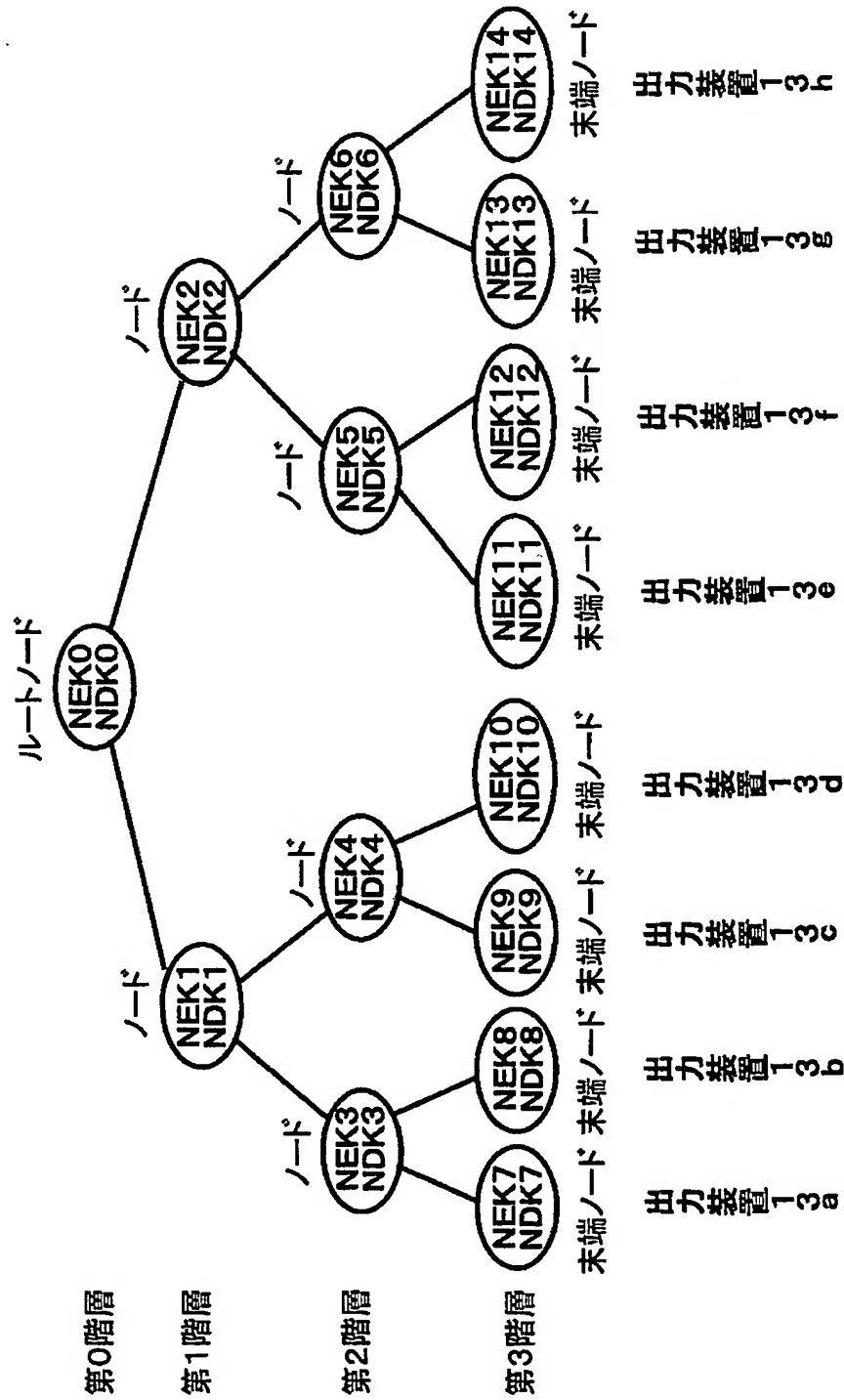
【図 1】

コンテンツ限定配信システム1

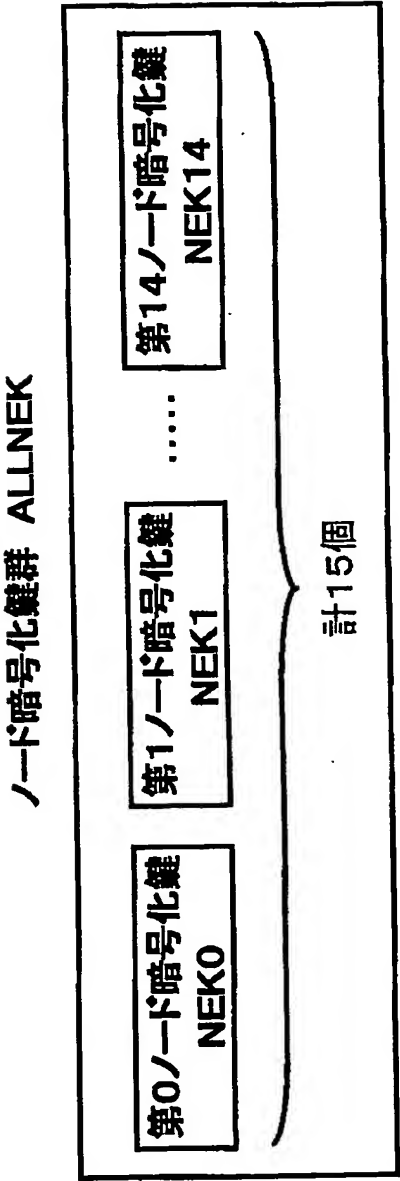


【図 2】

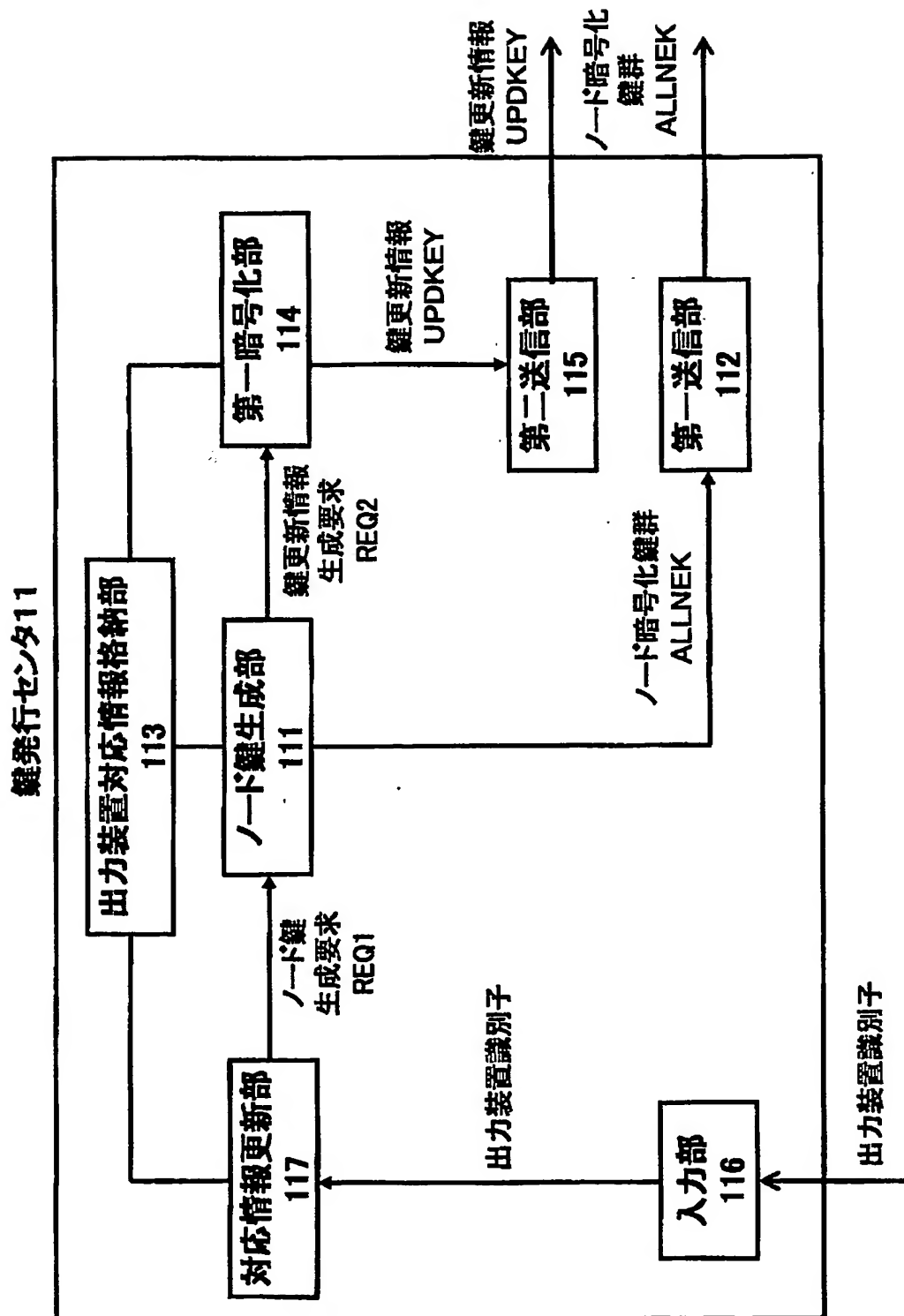
出力装置13a~13hに対するノード暗号化鍵及びノード復号化鍵の設定方法の一例



【図 3】

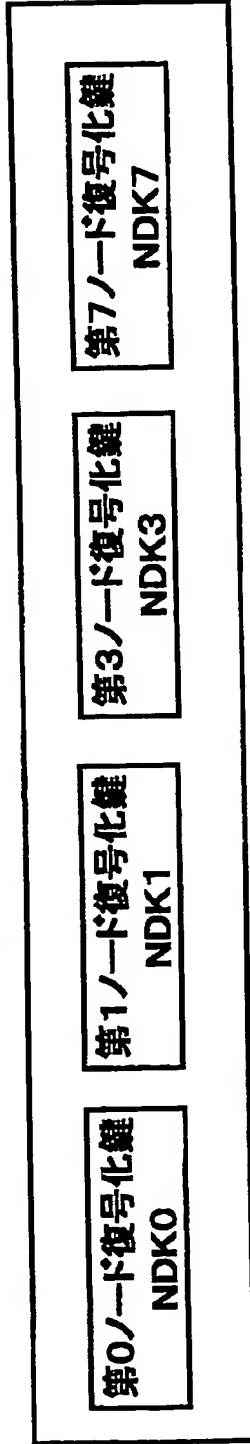


【図 4】



【図 5】

割当ノード復号化鍵群(出力装置13a向け) ANDKGa



【図 6】

出力装置対応情報格納部113

出力装置識別子 AIDa	個別鍵 IKa	割当ノード復号化鍵群 ANDKGa
出力装置識別子 AIDb	個別鍵 IKb	割当ノード復号化鍵群 ANDKGb
・ ・	・ ・	・ ・
出力装置識別子 AIDh	個別鍵 IKh	割当ノード復号化鍵群 ANDKGh

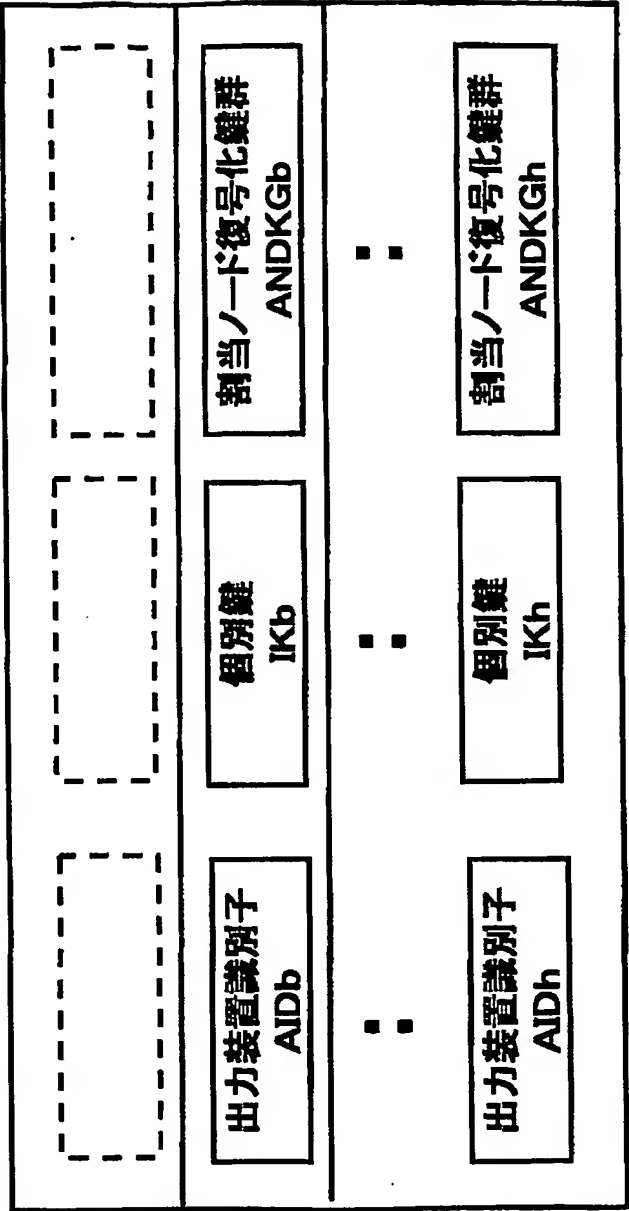
【図 7】

## 鍵更新情報 UPDKEY

出力装置識別子 AIDa	暗号化割当ノード復号化鍵群 ENCANDKGa
出力装置識別子 AIDb	暗号化割当ノード復号化鍵群 ENCANDKGb
⋮	⋮
出力装置識別子 AIDh	暗号化割当ノード復号化鍵群 ENCANDKGh

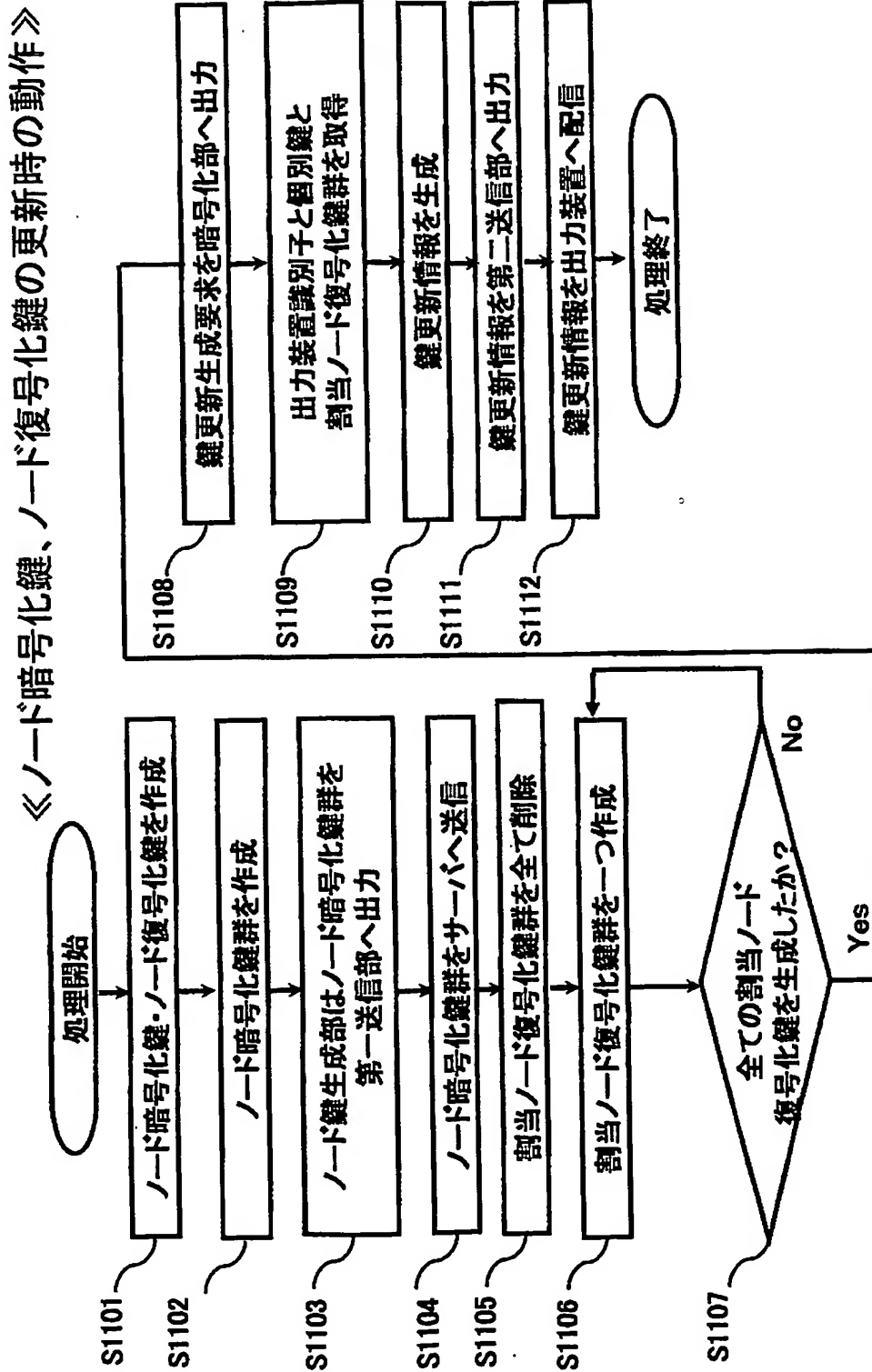
【図 8】

出力装置対応情報格納部113（出力装置13a無効化後）



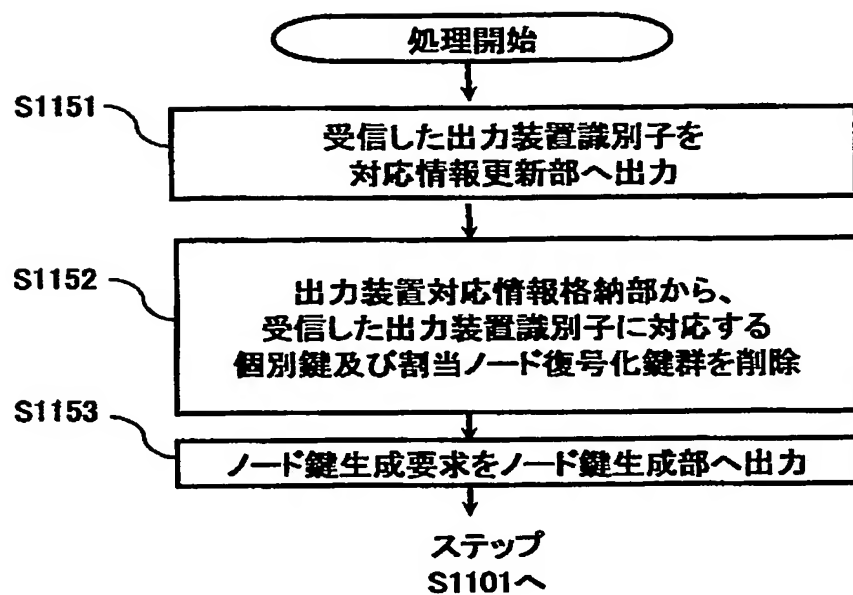


【図 9】

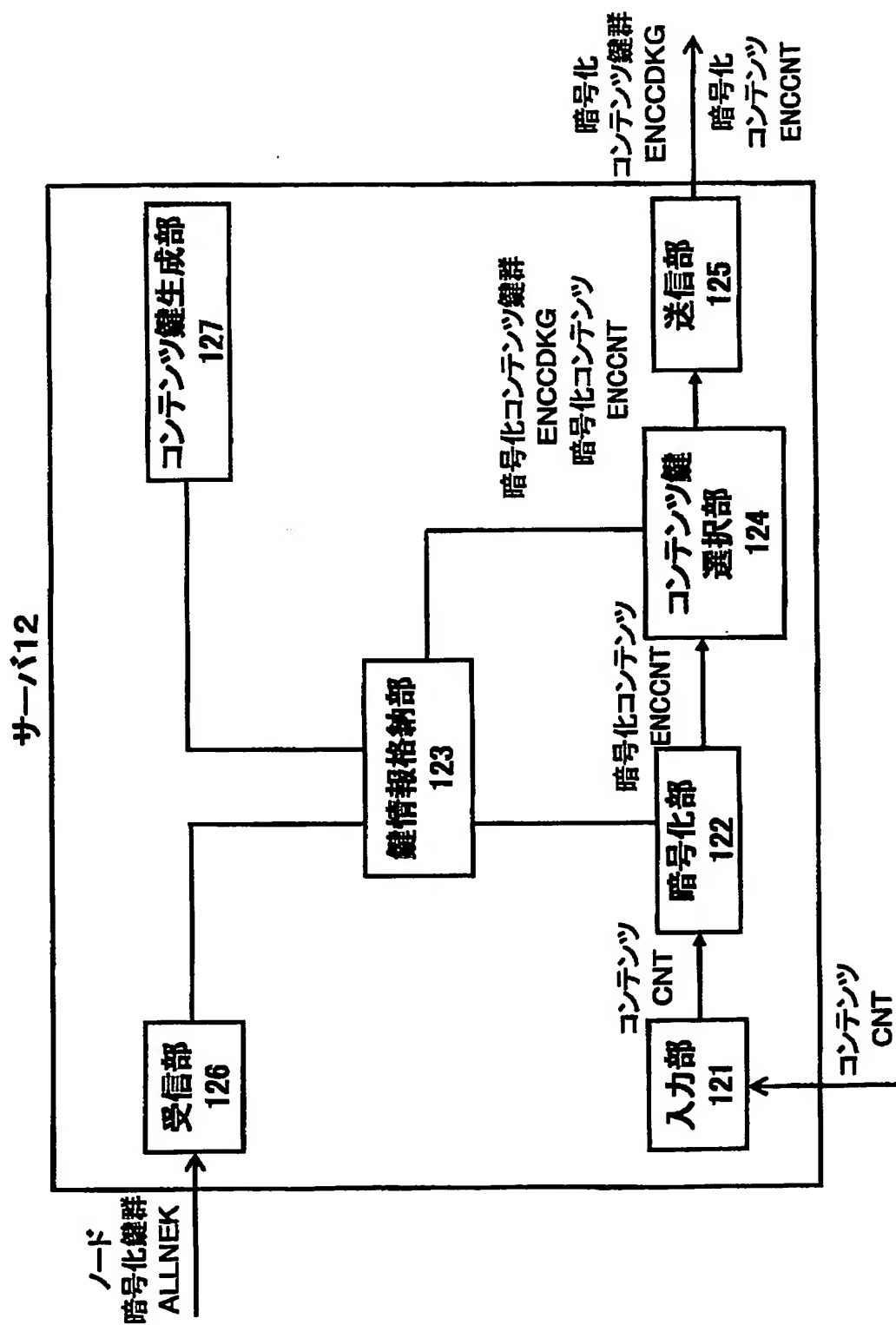


【図10】

## 《出力装置13aを無効化する動作》

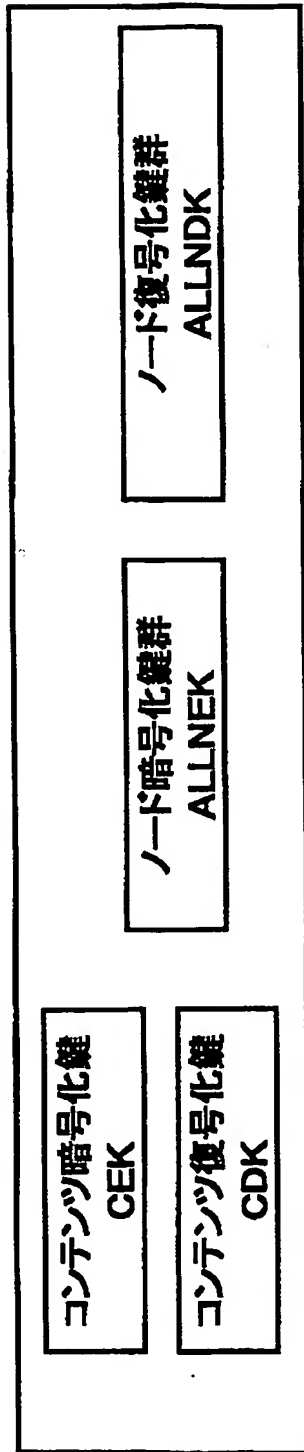


【図 11】

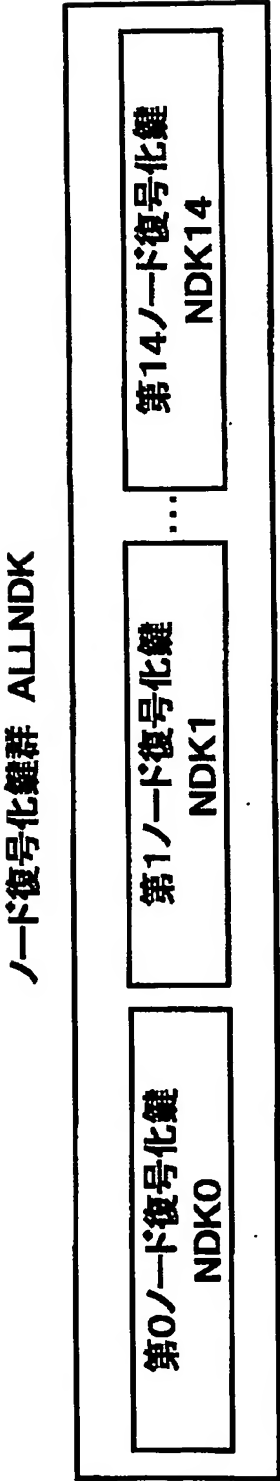


【図 12】

鍵情報格納部 123

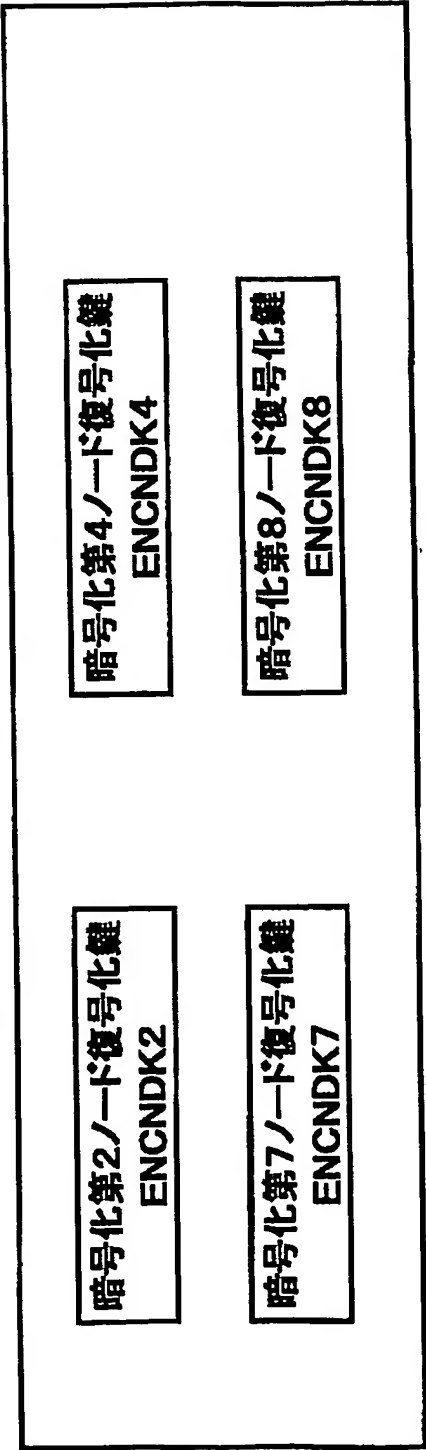


【図 13】

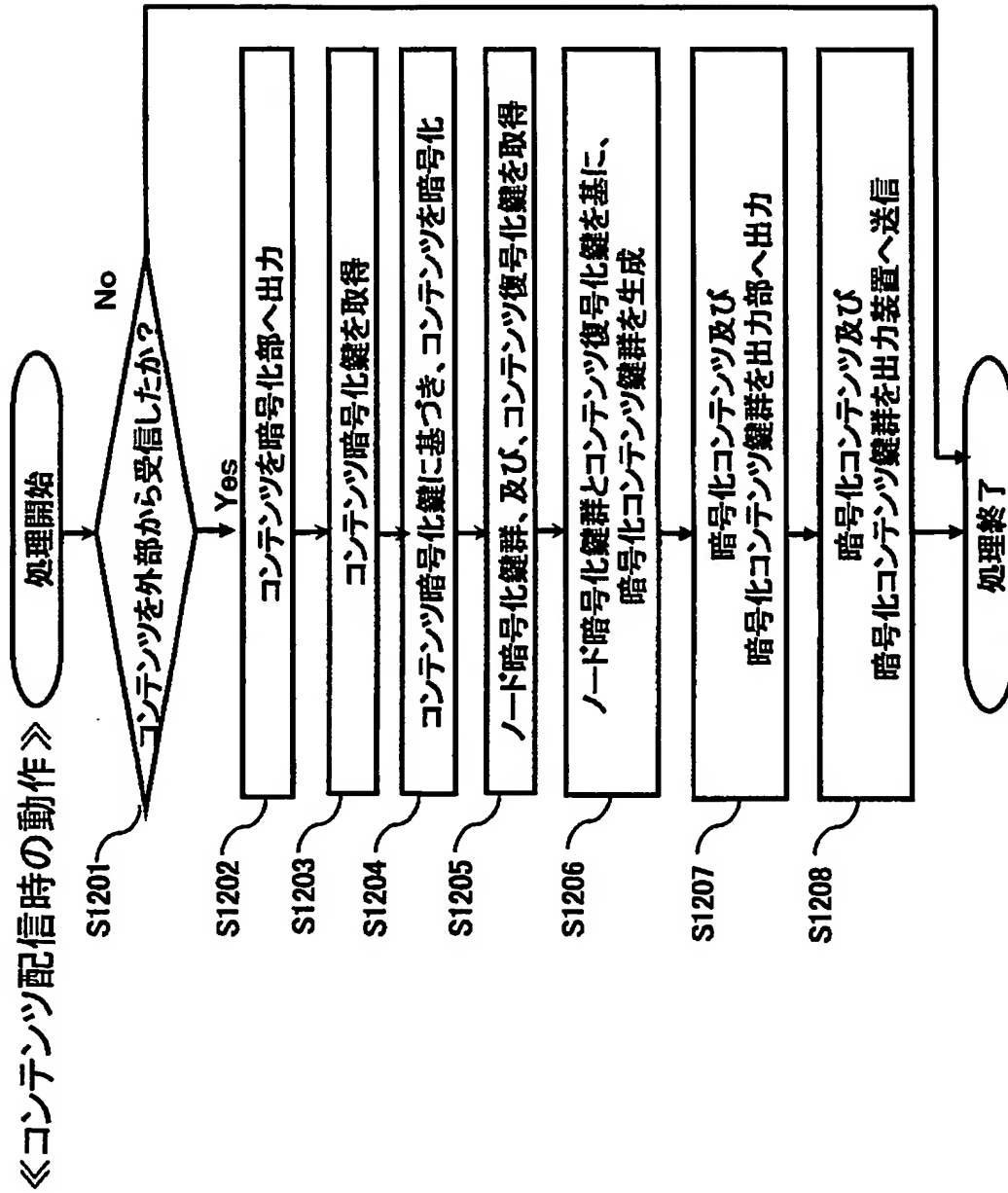


【図 14】

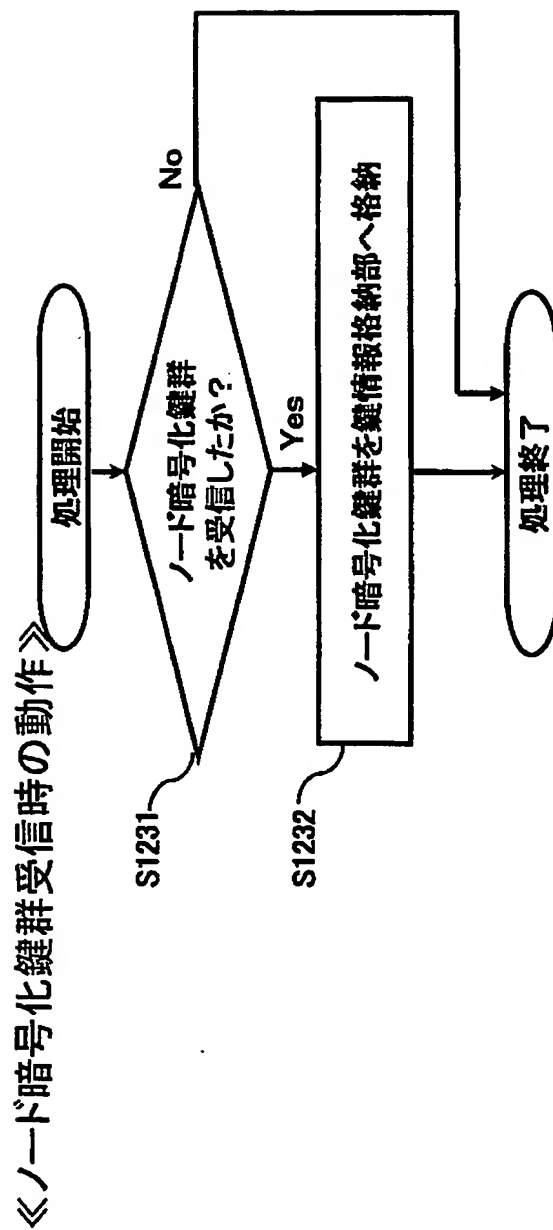
暗号化コンテンツ鍵群 ENCNDKG の例



【図 15】

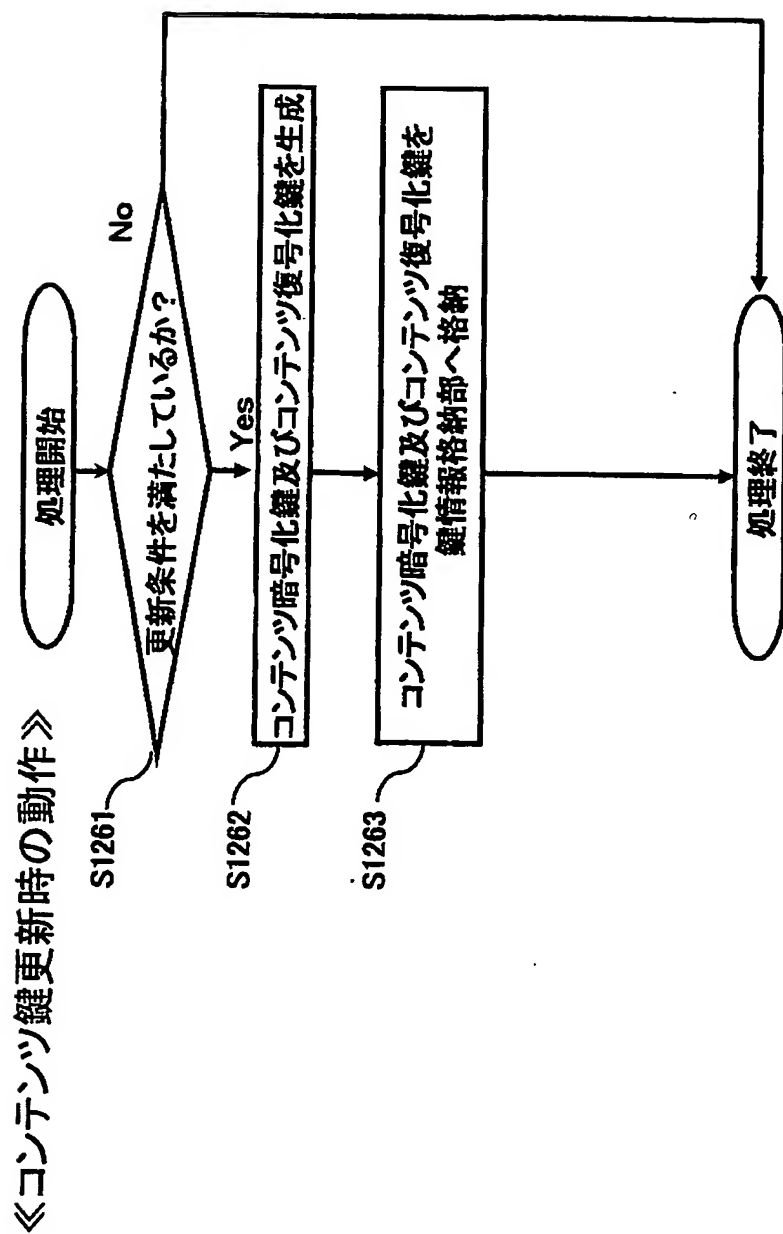


【図 16】

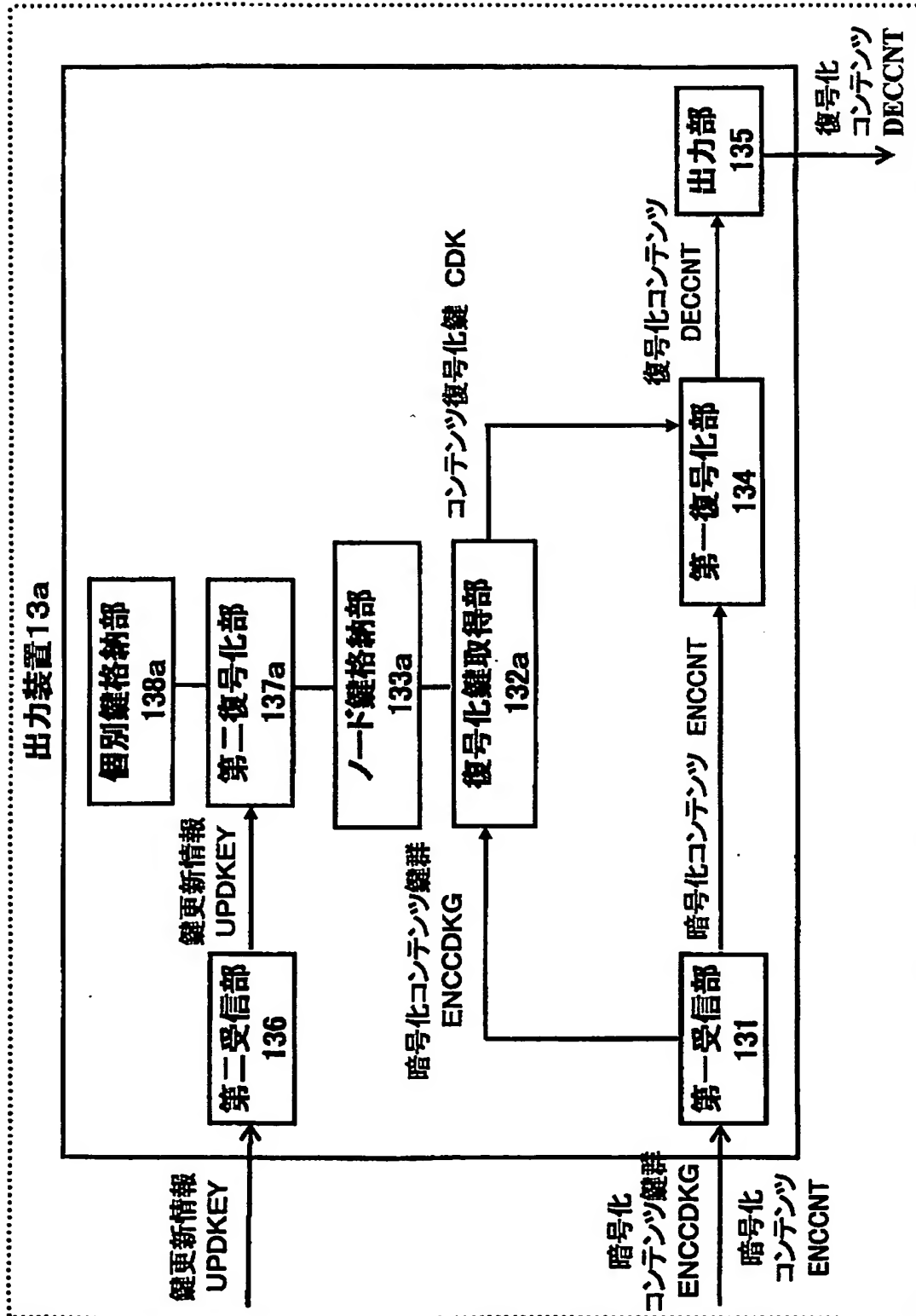




【図 17】



【図 18】



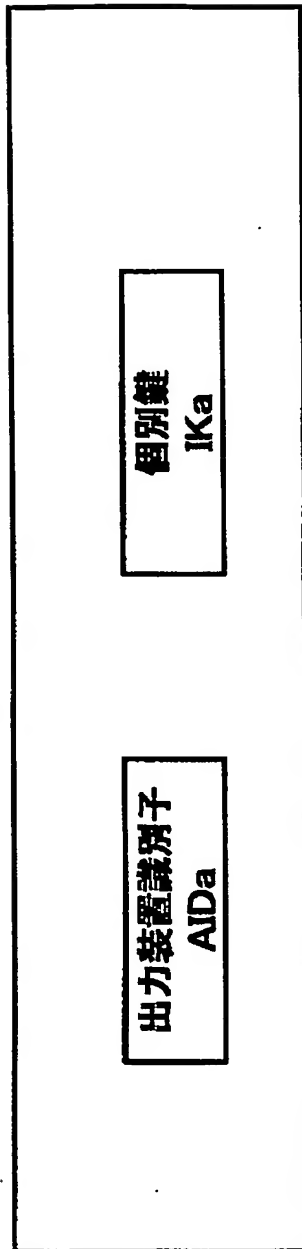
【図 19】

ノード鍵格納部133a

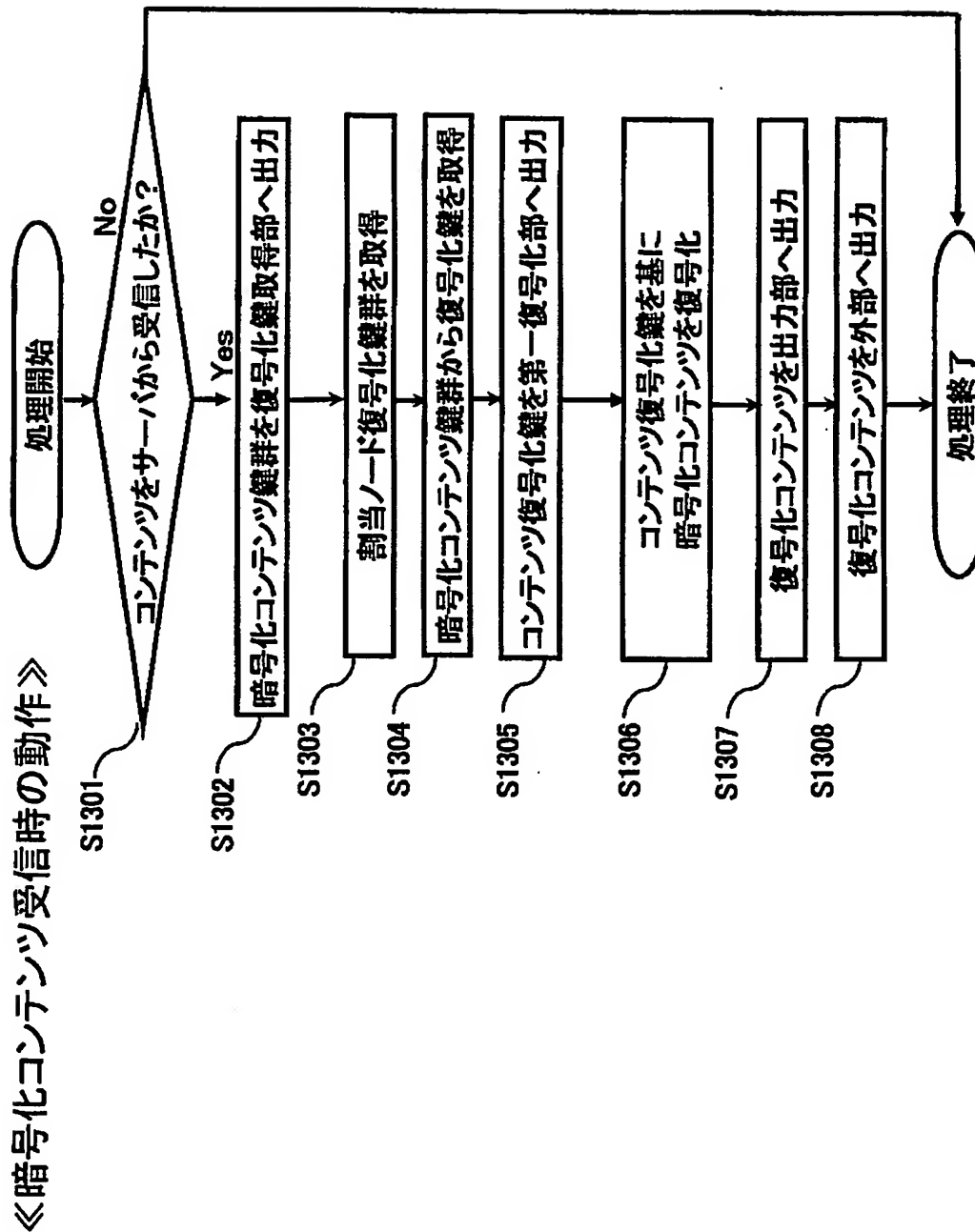
割当ノード復号化鍵群  
ANDKGa

【図 2 0】

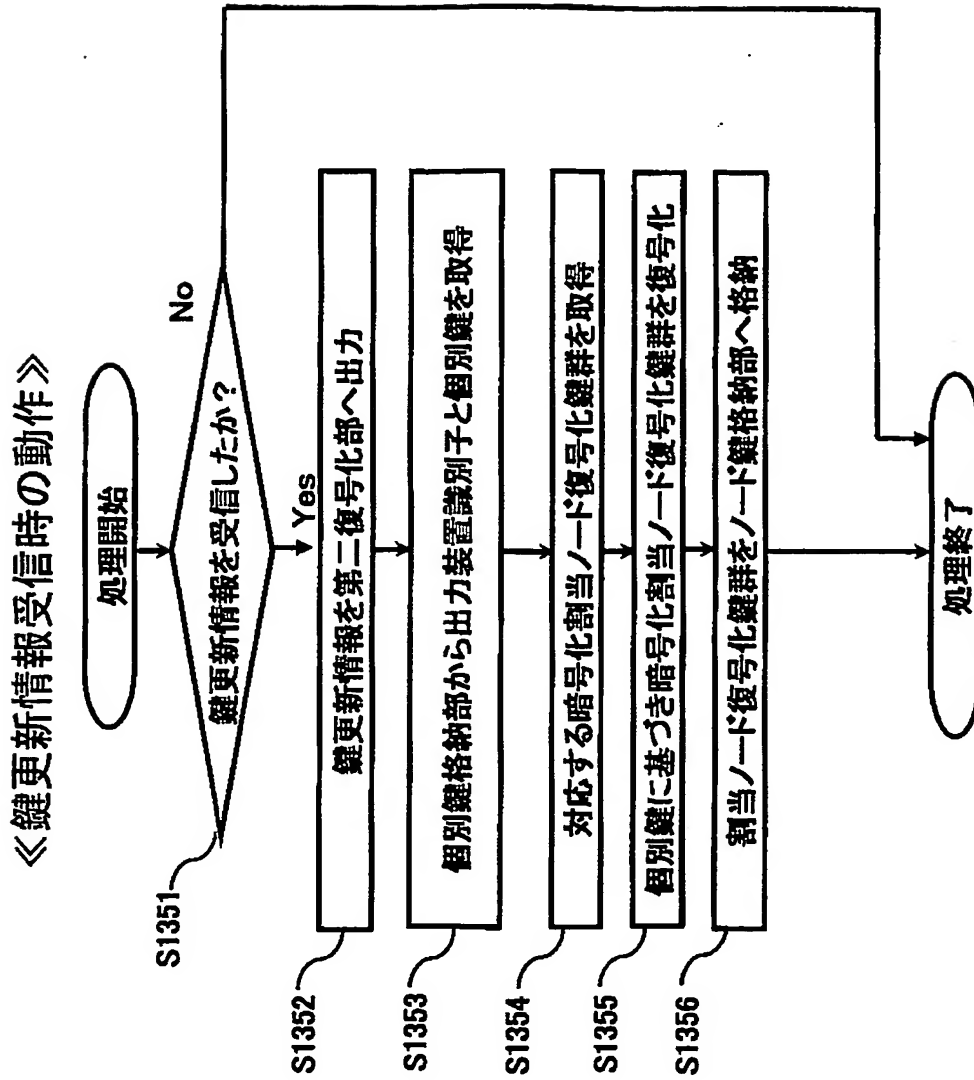
個別鍵格納部 138a



【図 21】

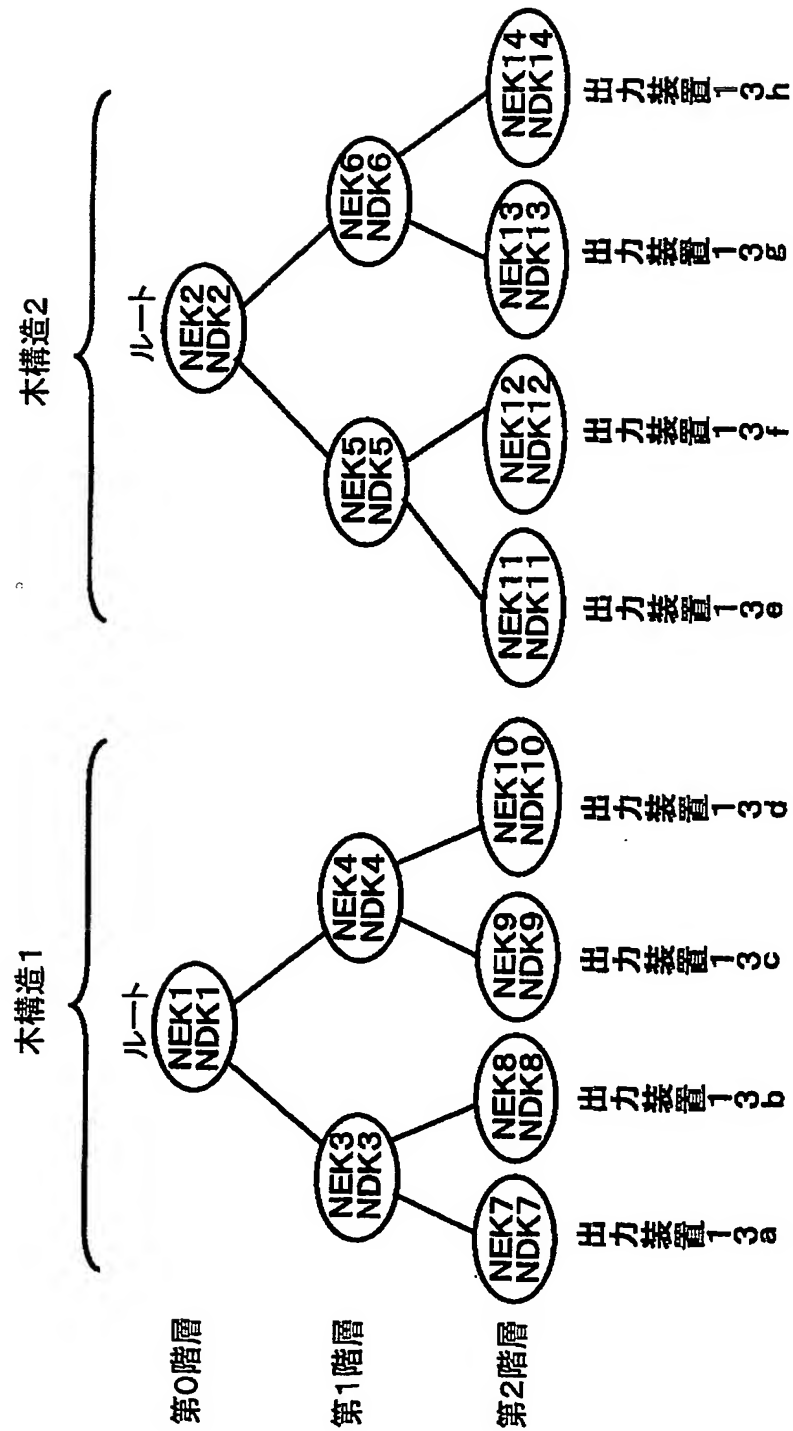


【図 22】



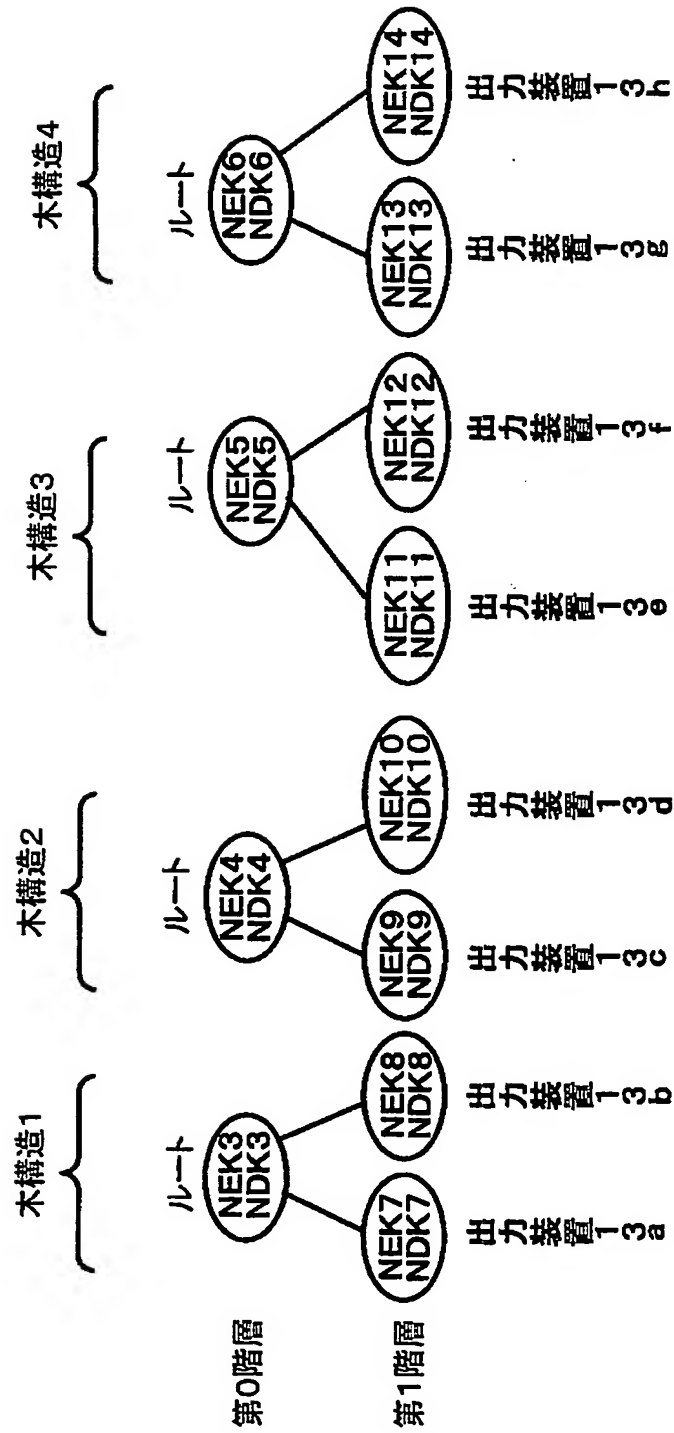
【図 23】

出力装置13a~13hに対するノード暗号化鍵及びノード復号化鍵の設定方法の別の一例



【図 24】

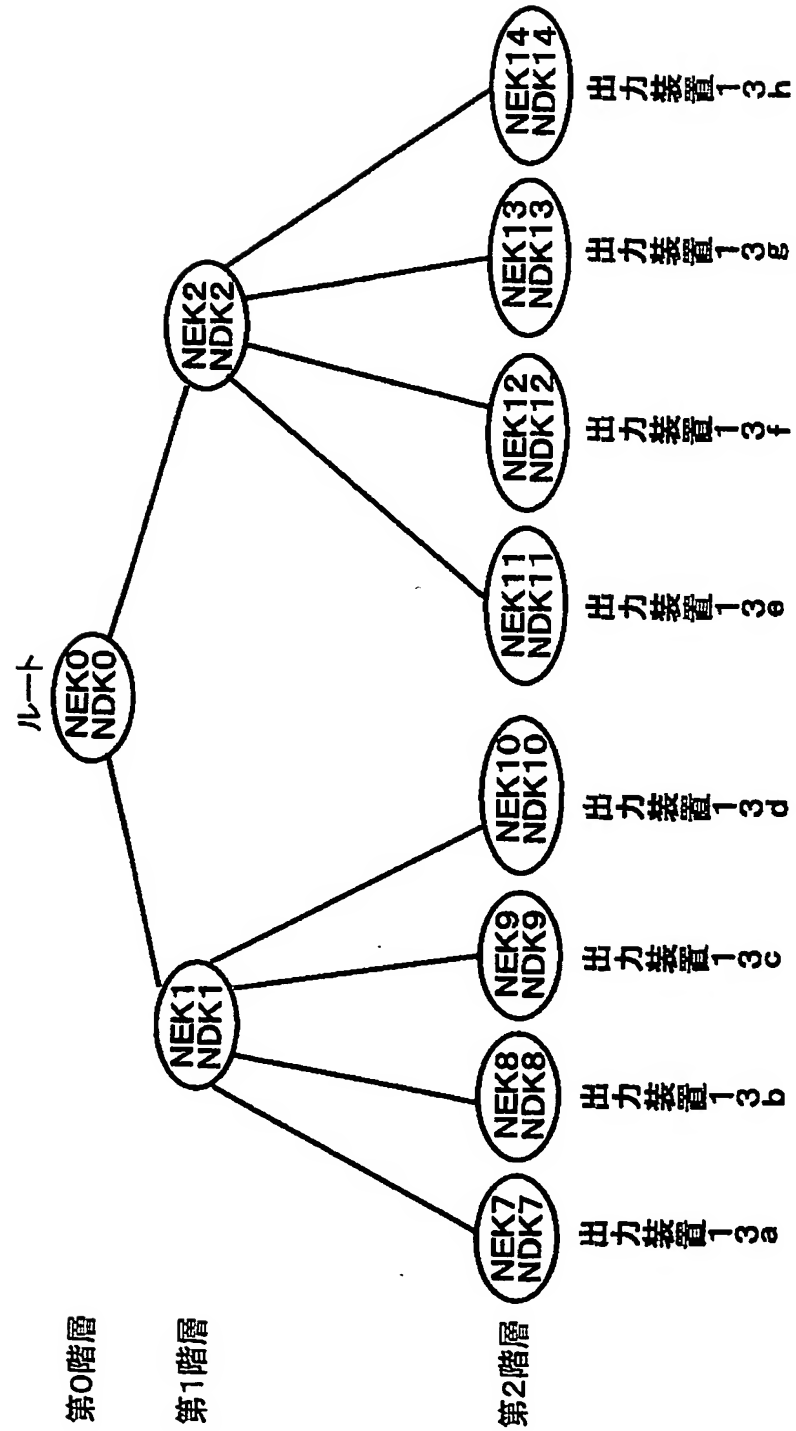
出力装置13a~13hに対するノード暗号化鍵及びノード復号化鍵の設定方法の別の一例





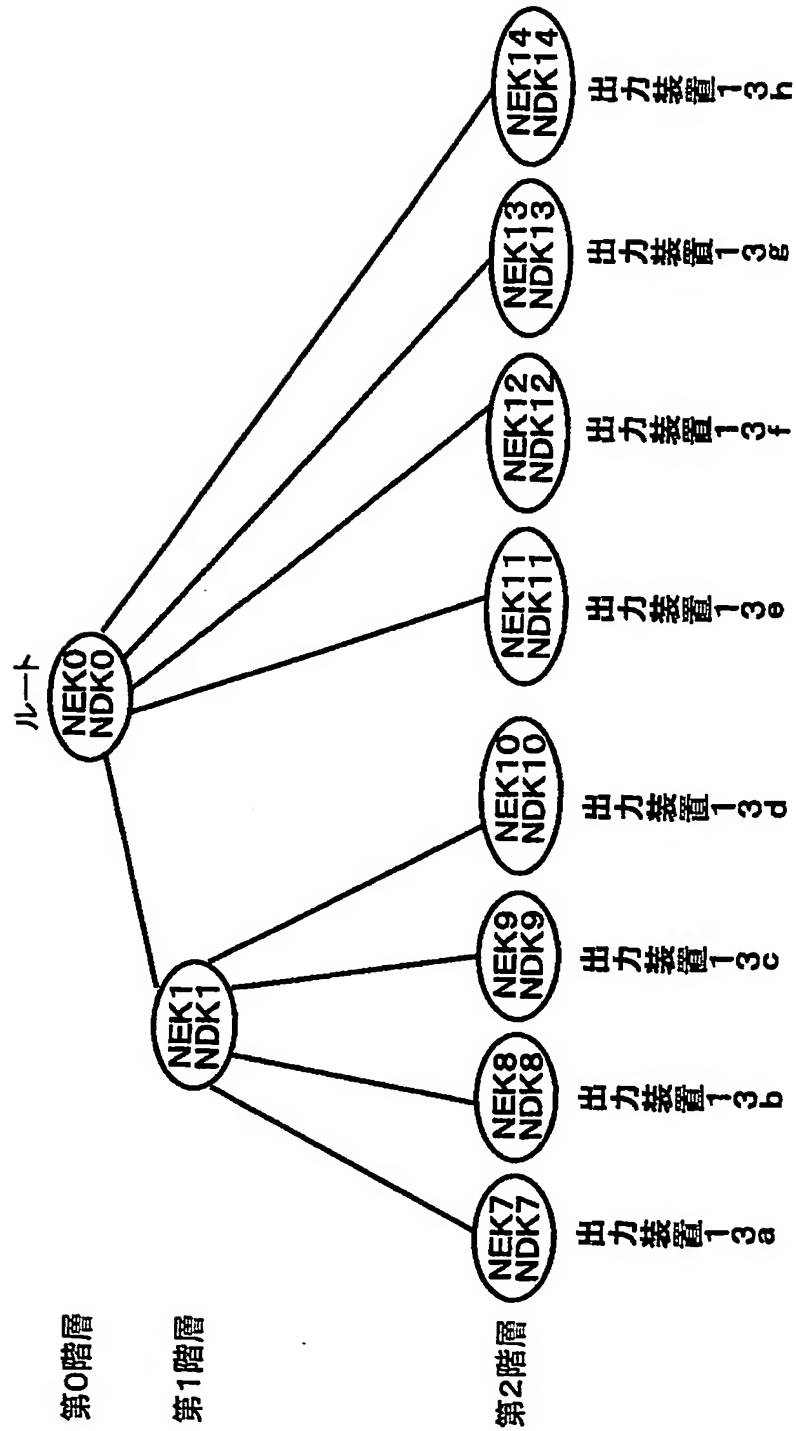
【図 25】

出力装置13a~13hに対するノード暗号化鍵及びノード復号化鍵の設定方法の別の一例



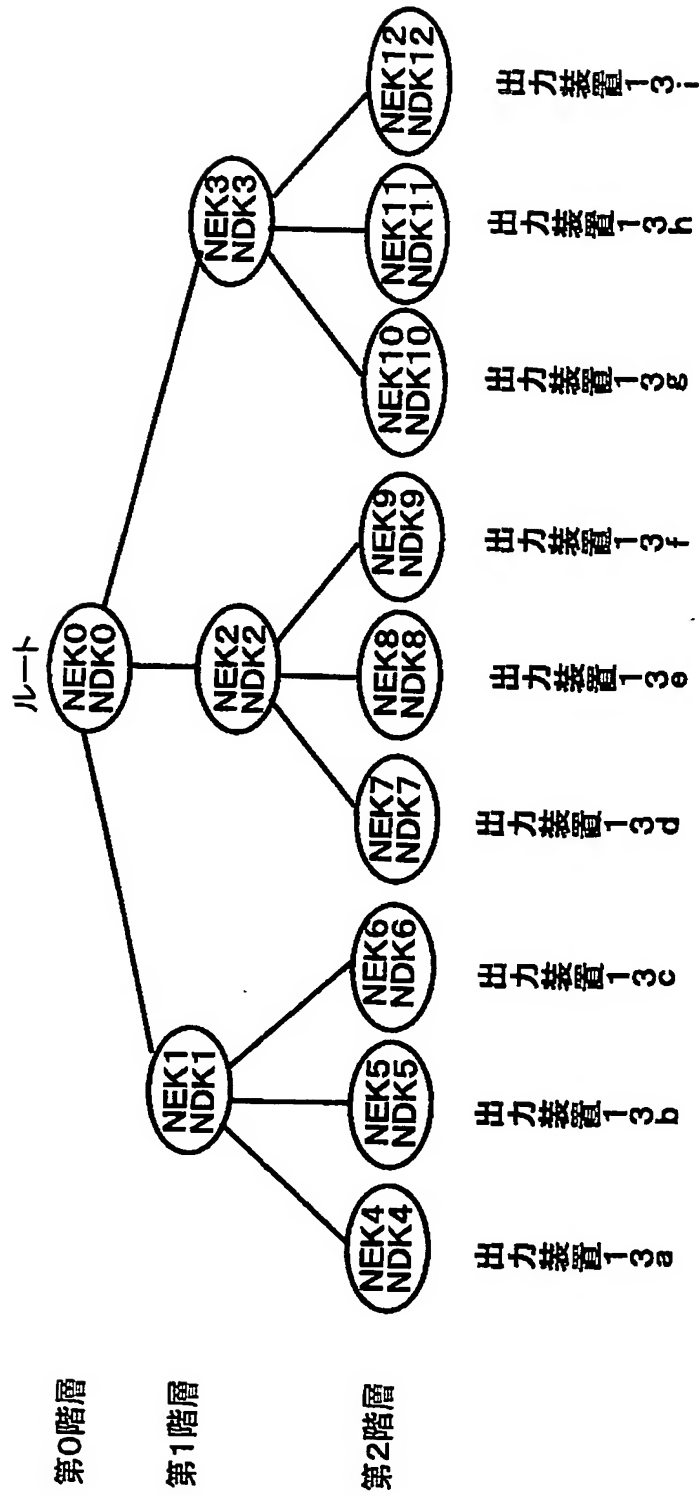
【図 26】

出力装置13a~13hに対するノード暗号化鍵及びノード復号化鍵の設定方法の別の一例



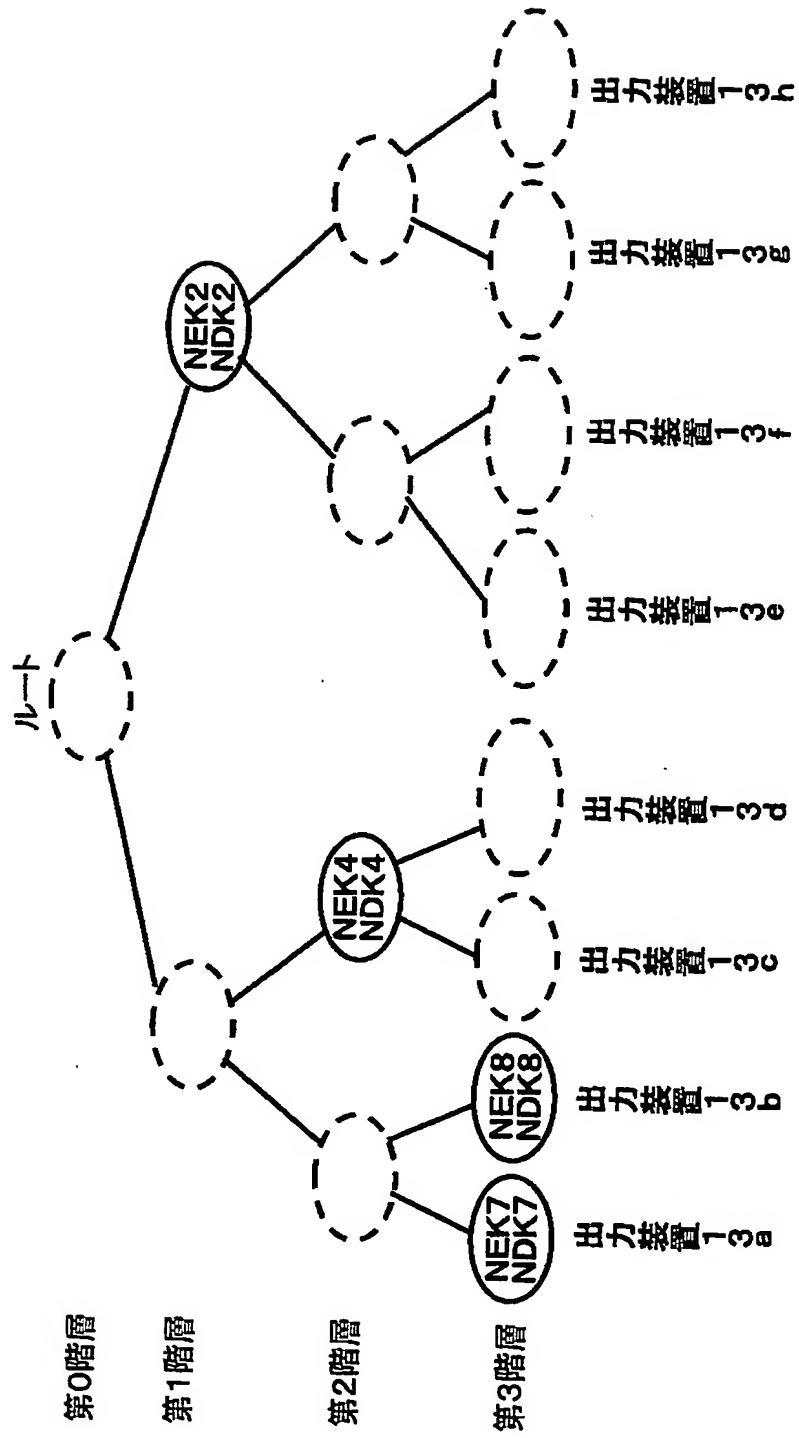
【図 27】

出力装置 13a~13h に対するノード暗号化鍵及びノード復号化鍵の設定方法の別の一例



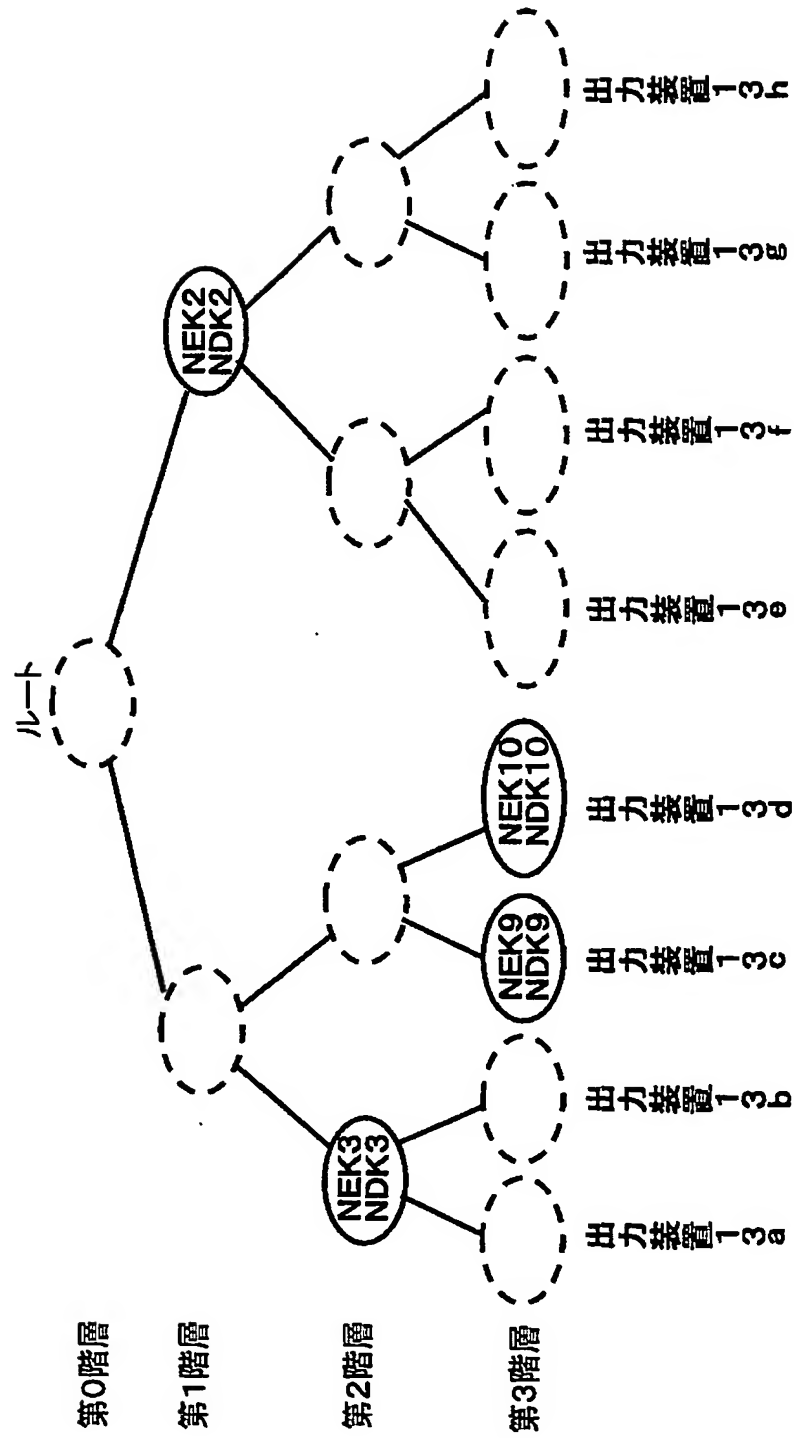
【図 28】

コンテンツ復号化鍵を暗号化するのに用いる複数のノード暗号化鍵の選定例（割当ノード復号化鍵群）



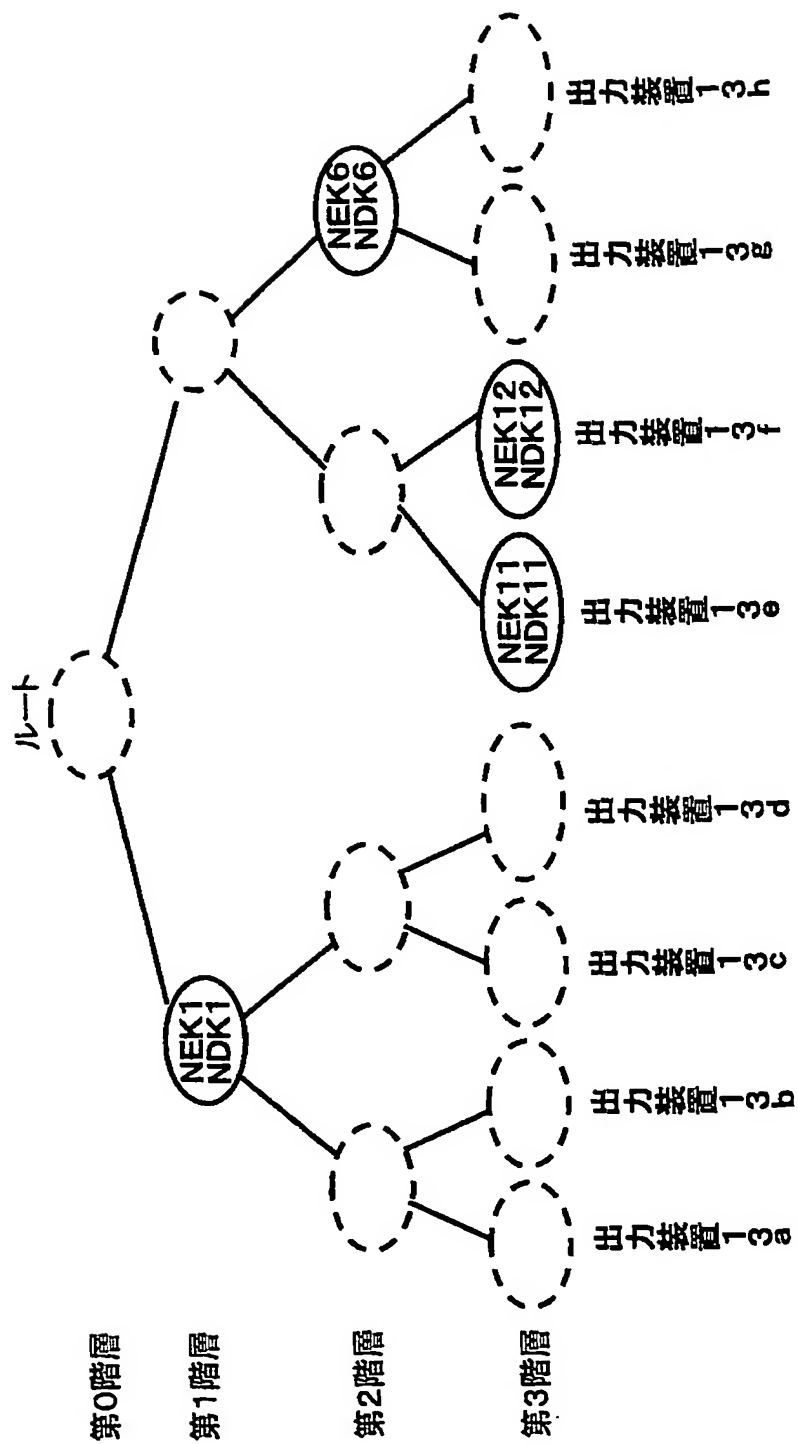
【図 29】

コンテンツ復号化鍵を暗号化するのに用いる複数のノード暗号化鍵の選定例 (割当ノード復号化鍵群)



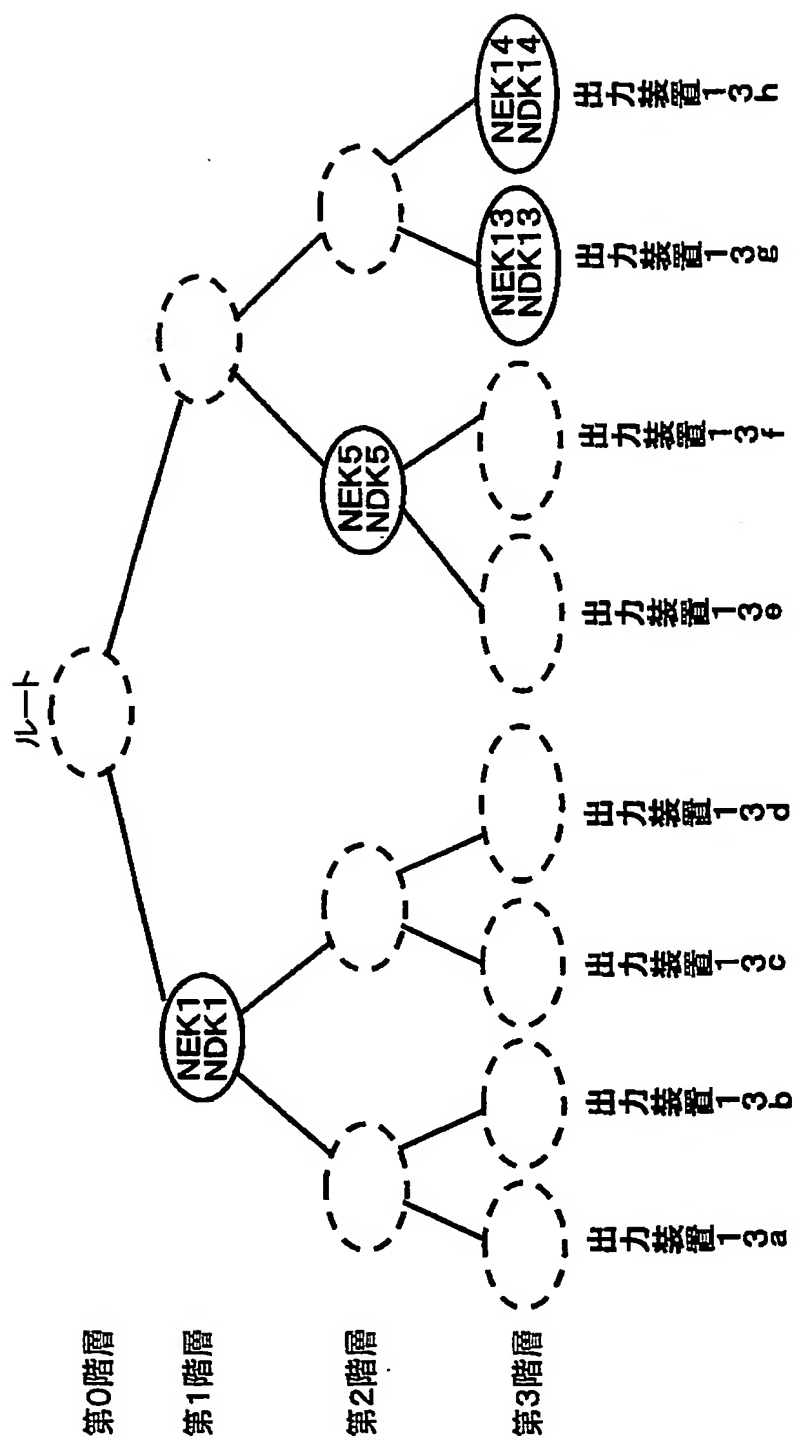
【図30】

コンテンツ復号化鍵を暗号化するのに用いる複数のノード暗号化鍵の選定例 (割当ノード復号化鍵群)



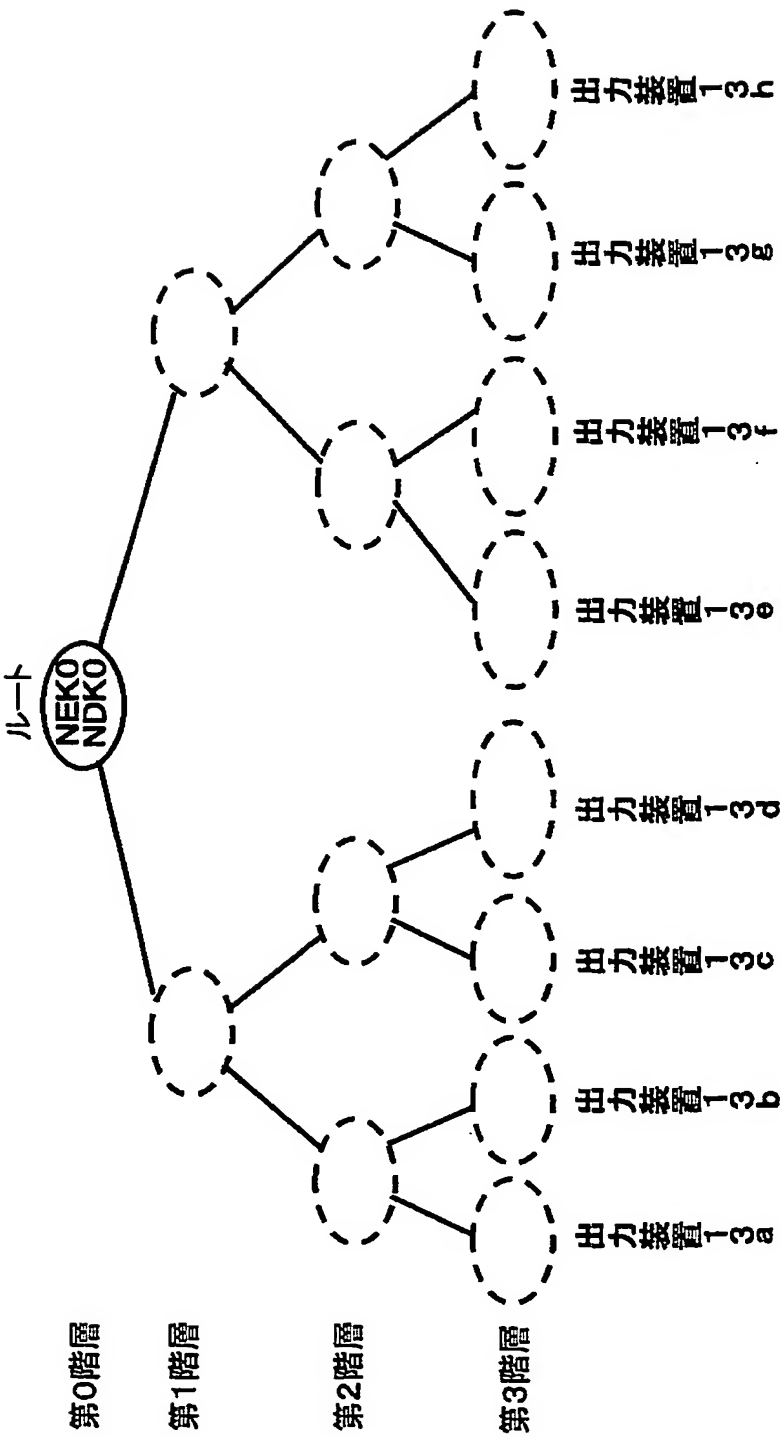
【図 31】

コンテンツ復号化鍵を暗号化するのに用いる複数のノード暗号化鍵の選定例（割当ノード復号化鍵群）



【図 3 2】

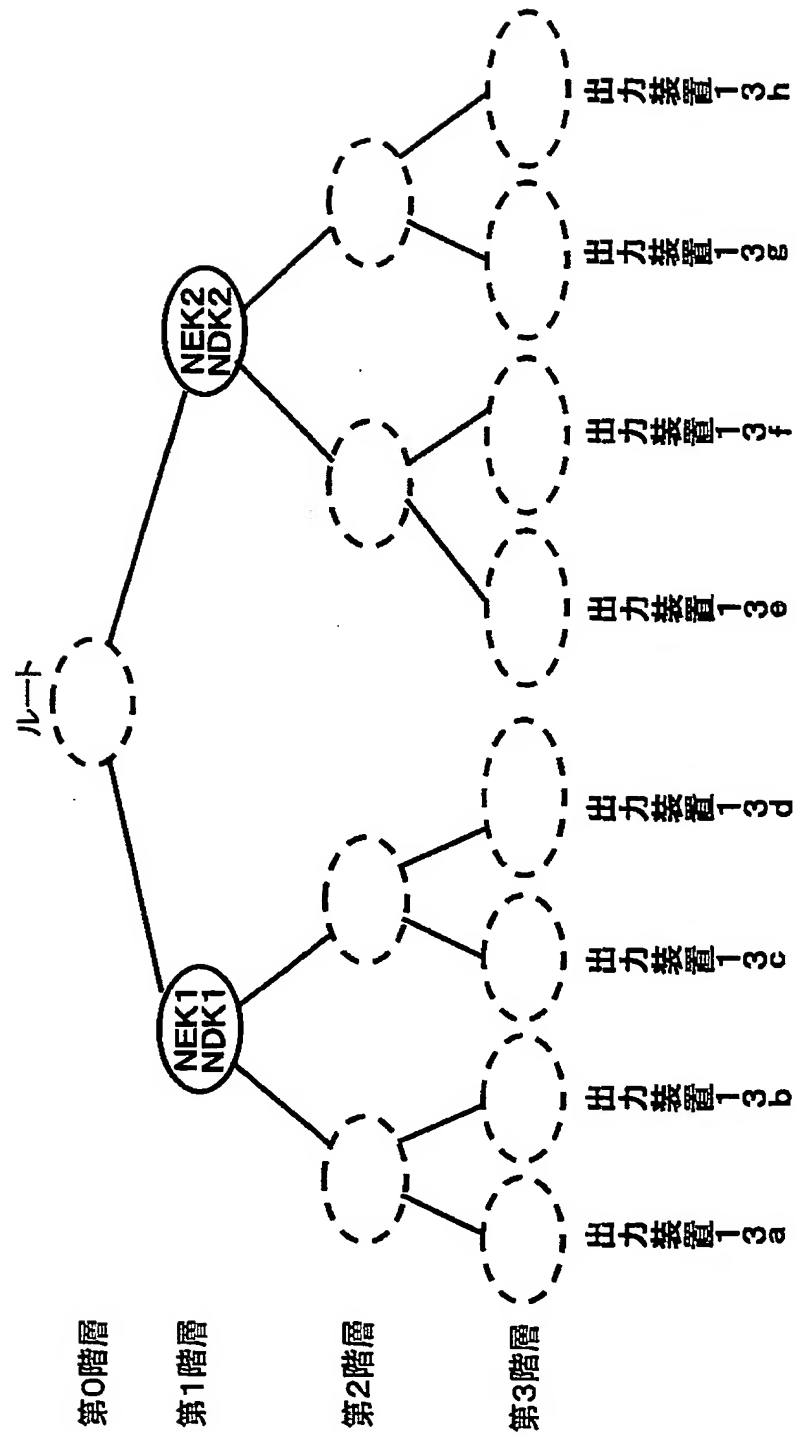
コンテンツ復号化鍵を暗号化するのに用いる複数のノード暗号化鍵の選定例（割当ノード復号化鍵群）





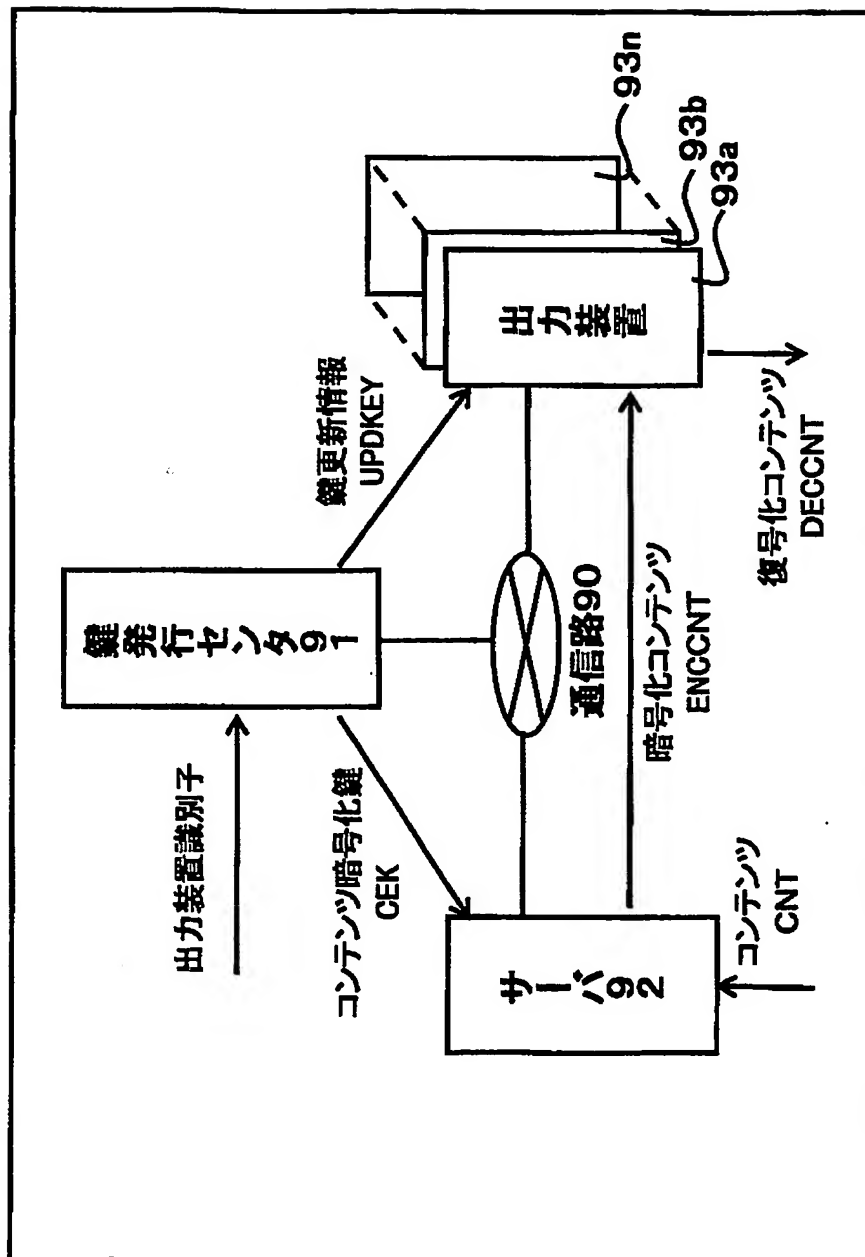
【図 33】

コンテンツ復号化鍵を暗号化するのに用いる複数のノード暗号化鍵の選定例 (割当ノード復号化鍵群)



【図 34】

従来のコンテンツ限定配信システム



## 【書類名】 要約書

## 【要約】

【課題】 コンテンツ鍵を更新する毎に送信する鍵更新用データサイズが大きかった。

【解決手段】 本発明は、コンテンツを配信するコンテンツ配信システムであって、鍵発行センタ 11 と、サーバ 12 と、8 台の出力装置 13 a ～ 13 h とが接続されている通信路 10 とから構成される。ここで、鍵発行センタ 11 と出力装置 13 a ～ 13 h の全ての組には、予め各々の組が共有している一つの個別鍵が与えられており、例えば鍵発行センタ 11 と出力装置 13 a は個別鍵 I K a を、鍵発行センタ 11 と出力装置 13 b は個別鍵 I K b を、鍵発行センタ 11 と出力装置 13 h は個別鍵 I K h を予め共有している。

【選択図】 図 1

認定・付加情報

特許出願の番号	特願 2003-419765
受付番号	50302078118
書類名	特許願
担当官	第三担当上席 0092
作成日	平成15年12月18日

<認定情報・付加情報>

【提出日】	平成15年12月17日
-------	-------------

特願 2 0 0 3 - 4 1 9 7 6 5

出 願 人 履 歴 情 報

識別番号

[ 0 0 0 0 0 5 8 2 1 ]

1. 変更年月日

1 9 9 0 年 8 月 2 8 日

[変更理由]

新規登録

住 所

大阪府門真市大字門真 1 0 0 6 番地

氏 名

松下電器産業株式会社

# Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP04/019124

International filing date: 15 December 2004 (15.12.2004)

Document type: Certified copy of priority document

Document details: Country/Office: JP  
Number: 2003-419765  
Filing date: 17 December 2003 (17.12.2003)

Date of receipt at the International Bureau: 10 February 2005 (10.02.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland  
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse